ADDITIVE COMBINATORICS METHODS IN ASSOCIATIVE ALGEBRAS

VINCENT BECK AND CÉDRIC LECOUVEY

Abstract. We adapt methods coming from additive combinatorics in groups to the study of linear span in associative unital algebras. In particular, we establish for these algebras analogues of Diderrich-Kneser's and Hamidoune's theorems on sumsets and Tao's theorem on sets of small doubling. In passing we classify the finite-dimensional algebras over infinite fields with finitely many subalgebras. These algebras play a crucial role in our linear version of Diderrich-Kneser's theorem. We also explain how the original theorems for groups we linearize can be easily deduced from our results applied to group algebras. Finally, we give lower bounds for the Minkowski product of two subsets in finite monoids by using their associated monoid algebras.

1. Introduction

In this paper, we first establish analogues of theorems in additive combinatorics on groups for a wide class of associative unital algebras. Next we explain how this algebra setting permits to recover the original results on groups and their analogues in fields but also yields similar lower bounds for the Minkowski product of two subsets in monoids. Our results and tools mix additive number theory, combinatorics, linear and commutative algebra and basics considerations on Banach algebras.

Given A and B two non empty sets of a given group G, a classical problem in additive combinatorics is to evaluate the cardinality $|AB|$ of the Minkowski product $AB = \{ab \mid a \in A, b \in B\}$ in terms of the cardinalities $|A|$ and $|B|$. There exists a wide literature on this subject, notably a famous result by Kneser (see [5], [14]).

Theorem 1.1 (Kneser)**.** *Let A and B be finite subsets of the* abelian *group G. Then*

$$|AB| \geq |A| + |B| - |H|$$

where $H = \{h \in G \mid hAB = AB\}$ is the stabilizer of AB in G.

This theorem does not hold for non abelian groups and the question of finding lower and upper bounds for product sets becomes then considerably more difficult. Nevertheless, there exist in this case numerous weaker results. Let us mention among them those of Diderrich [2], Olson [15] and Tao [17], [18] we shall evoke in more details in Section 4.

Analogous estimates exist in the context of fields and division rings. As far as we are aware, this kind of generalizations was considered for the first time in [6] and [9]. Consider K a field extension of the field k and A a finite subset in K. Write $\mathrm{k}\langle A\rangle$ for the k-subspace of K generated by A and let $\dim_{\mathrm{k}}(A)$ be its dimension. For A, B two finite subsets of K, we set $AB = \{ab \mid a \in A, b \in A\}$. Then $\dim_{\mathrm{k}}(AB)$, the dimension of $\mathrm{k}\langle AB\rangle$, is finite. The following analogue of Kneser's theorem for fields is proved in [6] and [9].

Theorem 1.2. *Let K be a commutative extension of* k*. Assume every algebraic element in K is separable over* k*. Let A and B be two nonempty finite subsets of K^*. Then*

$$\dim_{\mathrm{k}}(AB) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B) - \dim_{\mathrm{k}}(H) \tag{1}$$

Date: June, 2015.

where $H := \{h \in K \mid h\mathrm{k}\langle AB\rangle \subseteq \mathrm{k}\langle AB\rangle\}$.

Here H is an intermediate field containing k and the separability hypothesis is crucial since the proof uses the fact that K admits only a finite number of finite extensions of k (which is also assumed in [9]). Equivalently, this theorem asserts that the sum of the dimensions of $\mathrm{k}\langle AB\rangle$ and its stabilizer must be at least equal to the sum of dimensions of $\mathrm{k}\langle A\rangle$ and $\mathrm{k}\langle B\rangle$. Remarkably, the authors showed that their theorem implies Kneser's theorem for abelian groups by using Galois correspondence. Observe it is not known if the theorem remains valid without the separability hypothesis (see [8]). Non commutative analogues of this theorem were established in [3] (linear version of Olson's theorem without any separability hypothesis) and in [12] (linear version of Diderrich's theorem where only the elements of the set A are assumed pairwise commutative).

In [12], linear analogues (i.e. in division rings and fields) of theorems by Plünnecke and Ruzsa [16] are given yielding upper bounds for $\dim_{\mathrm{k}}(AB)$. In passing we observe these theorems can be adapted to some unital associative algebras. It is then a natural question to ask wether lower bound estimates for $\dim_{\mathrm{k}}(AB)$ similar to (1) exists for subspaces of a unital associative k-algebra $\mathcal{A}$. A first obstruction is due to the existence of non trivial annihilators of subsets. Indeed if the right annihilator $\mathrm{ann}_r(A)$ of A is not reduced to $\{0\}$, we can take for B any generating subset of $\mathrm{ann}_r(A)$ and obtain $\dim_{\mathrm{k}}(AB) = 0$. To overcome this problem, we will assume most of the time that the k-subspaces we consider in $\mathcal{A}$ contains at least one invertible element. We thus have $\mathrm{ann}_r(\mathrm{k}\langle A\rangle) = \mathrm{ann}_l(\mathrm{k}\langle A\rangle) = \{0\}$. We prove in this paper that, quite surprisingly, this suffices to establish in $\mathcal{A}$ an analogue of Diderrich's theorem but also analogues of estimates by Hamidoune and Tao. To obtain lower bounds similar to (1), it nevertheless remains a second obstruction. We indeed need an analogue of the separability hypothesis in our algebras context. In fact we shall see that it suffices to assume that the subalgebra of $\mathcal{A}$ generated by A has finitely many finite-dimensional subalgebras. This leads us to classify the f.d. associative unital algebras with finitely many subalgebras in Section 3.

The Paper is organized as follows. In Section 2 we precise the algebra setting we consider. Also to get a sufficient control on the invertible elements of the algebra $\mathcal{A}$, we need to assume in the theorems we establish that k is infinite and $\mathcal{A}$ satisfies one of the two following (strong or weak) hypotheses:

- $\mathbf{H}_{\mathrm{s}}$**:** $\mathcal{A}$ is finite-dimensional over k or a Banach algebra or a finite product of (possibly infinite-dimensional) field extensions over k.
- $\mathbf{H}_{\mathrm{w}}$**:** $\mathcal{A}$ is finite-dimensional over k or a subalgebra of a Banach algebra or a subalgebra of a finite product of (possibly infinite-dimensional) field extensions over k. Equivalently, an algebra verifying $\mathbf{H}_{\mathrm{w}}$ is a subalgebra of an algebra verifying $\mathbf{H}_{\mathrm{s}}$.

These hypotheses are not optimal and one can establish some refinements of our results we will not detail for simplicity. The main result of Section 3 is the classification of f.d algebras with finitely many subalgebras. Section 4 is devoted to the analogue of Diderrich's theorem. We notably obtain a lower bound similar to (1) where $\mathcal{H}$ is the subalgebra of $\mathcal{A}$ which stabilizes $\mathrm{k}\langle AB\rangle$. In Section 5, we establish analogues of results by Tao on spaces of small doubling using a linear version of Hamidoune connectivity. Finally, in Section 6, we explain how the original theorems of Kneser and Diderrich in a group G can be very easily recovered from our linear version in the group algebra of G. In particular, the link with the group setting does not require to realize G as the Galois group of a finite extension of k as in [6] which would become problematic when G is non abelian. We also explain, in Section 7, how it is possible to state Hamidoune type results in finite monoids by considering their monoid algebras.

While writing this paper, we were informed by G. Zémor that a Kneser type theorem has been very recently obtained in [13] for the algebra $\mathcal{A} = \mathrm{k}^n$ with applications to linear code theory.

Acknowledgments. Both authors are partly supported by the "Agence Nationale de la Recherche" grant ANR-12-JS01-0003-01 ACORT.

2. The algebra setting

2.1. **Vector span in an algebra.** Let $\mathcal{A}$ be a unital associative algebra over the field k. We denote by $\mathcal{A}_* = \mathcal{A} \setminus \{0\}$ and by $U(\mathcal{A})$ the group of invertible elements in $\mathcal{A}$. All along this paper, by a subalgebra $\mathcal{B}$ of $\mathcal{A}$, we always mean a unital subalgebra which contains 1.

For any subset A of $\mathcal{A}$, let $\mathrm{k}\langle A\rangle$ be the k-subspace of $\mathcal{A}$ generated by A. We write $|A|$ for the cardinality of A, and $\dim_{\mathrm{k}}(A)$ for the dimension of $\mathrm{k}\langle A\rangle$ over k. When $|A|$ is finite, $\dim_{\mathrm{k}}(A)$ is also finite and we have $\dim_{\mathrm{k}}(A) \leq |A|$. We denote by $\mathbb{A}(A) \subseteq \mathcal{A}$ the subalgebra generated by A in $\mathcal{A}$.

Given subsets A and B of $\mathcal{A}$, we thus have $\mathrm{k}\langle A \cup B\rangle = \mathrm{k}\langle A\rangle + \mathrm{k}\langle B\rangle$, the sum of the two spaces $\mathrm{k}\langle A\rangle$ and $\mathrm{k}\langle B\rangle$. We have also $\mathrm{k}\langle A \cap B\rangle \subseteq \mathrm{k}\langle A\rangle \cap \mathrm{k}\langle B\rangle$ and $\mathrm{k}\langle AB\rangle = \mathrm{k}\langle \mathrm{k}\langle A\rangle \mathrm{k}\langle B\rangle\rangle$. We write as usual

$$AB := \{ab \mid a \in A, b \in B\}$$

for the Minkowski product of the sets A and B. Given a family of nonempty subsets $A_1, \dots, A_n$ of $\mathcal{A}$, we define the Minkowski product $A_1 \cdots A_n$ similarly.

Any finite-dimensional k-subspace V of $\mathcal{A}$ can be realized as $V = \mathrm{k}\langle A\rangle$, where A is any finite subset of nonzero vectors spanning V. Also, when V_1 and V_2 are two k-vector spaces in K, $V_1V_2 \subseteq \mathrm{k}\langle V_1V_2\rangle$ but V_1V_2 is not a vector space in general. We set $U(V) := V \cap U(\mathcal{A})$ and $U(V)^{-1} = \{x^{-1} \mid x \in U(V)\}$. In what follows we denote by A, B subsets of $\mathcal{A}$ whereas V, W refer to k-subspaces of $\mathcal{A}$.

We aim to give some estimates of $\dim_{\mathrm{k}}(AB)$ in terms of $\dim_{\mathrm{k}}(A)$, $\dim_{\mathrm{k}}(B)$ and structure constants depending on the algebra $\mathcal{A}$ (typically the dimensions of some finite-dimensional subalgebras of $\mathcal{A}$). More generally we consider similar problems for $\dim_{\mathrm{k}}(A_1 \cdots A_r)$ where $A_1, \dots, A_r$ are finite subsets of $\mathcal{A}$. The following is straightforward

$$\max(\dim_{\mathrm{k}}(A), \dim_{\mathrm{k}}(B)) \leq \dim_{\mathrm{k}}(AB) \leq \dim_{\mathrm{k}}(A) \dim_{\mathrm{k}}(B)$$

when $\mathrm{k}\langle A\rangle$ and $\mathrm{k}\langle B\rangle$ contain at least an invertible element. In the sequel, we will restrict ourselves for simplicity to the case where k is infinite. For k a finite field, we can obtain estimates for $\dim_{\mathrm{k}}(AB)$ from the infinite field case by considering the algebra $\mathcal{A}' = \mathcal{A} \otimes_{\mathrm{k}} \mathrm{k}(t)$ where $\mathrm{k}(t)$ is field of rational functions in t over k. We indeed then have

$$\dim_{\mathrm{k}}(AB) = \dim_{\mathrm{k}(t)}(A'B'), \quad \dim_{\mathrm{k}}(A) = \dim_{\mathrm{k}(t)}(A') \quad \text{and} \quad \dim_{\mathrm{k}}(B) = \dim_{\mathrm{k}(t)}(B')$$

where $A' = A \otimes_{\mathrm{k}} 1 \in \mathcal{A} \otimes \mathrm{k}(t)$ and $B' = B \otimes_{\mathrm{k}} 1 \in \mathcal{A} \otimes \mathrm{k}(t)$. The following elementary lemma will be useful.

Lemma 2.1. *Let $\mathcal{A}$ be a finite-dimensional algebra over the field* k *and A be a finite subset of $\mathcal{A}$ such that $A \cap U(\mathcal{A}) \neq \emptyset$ and $\mathrm{k}\langle A^2\rangle = \mathrm{k}\langle A\rangle$. Then $\mathrm{k}\langle A\rangle$ is a subalgebra $\mathcal{A}$ of and $U(\mathrm{k}\langle A\rangle) = U(\mathcal{A}) \cap \mathrm{k}\langle A\rangle$.*

Proof. Observe that $\mathrm{k}\langle A^2\rangle = \mathrm{k}\langle A\rangle$ means that $\mathrm{k}\langle A\rangle$ is closed under multiplication. Then, for any nonzero $a \in \mathrm{k}\langle A\rangle$, the map $\varphi_a : \mathrm{k}\langle A\rangle \to \mathrm{k}\langle A\rangle$ which sends $\alpha \in \mathrm{k}\langle A\rangle$ on $\varphi_a(\alpha) = a\alpha$ is a k-linear endomorphism of the space $\mathrm{k}\langle A\rangle$. If we choose $a \in \mathrm{k}\langle A\rangle \cap U(\mathcal{A})$, φ_a is a k-linear injective endomorphism of the finite-dimensional space $\mathrm{k}\langle A\rangle$. Hence it is an automorphism. There then exists $\alpha \in \mathrm{k}\langle A\rangle$ such that $a\alpha = a$. Since $a \in U(\mathcal{A})$, this shows that $\alpha = 1 \in \mathrm{k}\langle A\rangle$ and $\mathrm{k}\langle A\rangle$

is a unital subalgebra of $\mathcal{A}$. Now since $1 \in \mathrm{k}\langle A\rangle$, there exists $\beta \in \mathrm{k}\langle A\rangle$ such that $a\beta = 1$. So $a^{-1} = \beta \in \mathrm{k}\langle A\rangle$ and $U(\mathrm{k}\langle A\rangle) = U(\mathcal{A}) \cap \mathrm{k}\langle A\rangle$. □

For any subset A in $\mathcal{A}_*$, we set

$$\mathcal{H}_l(A) := \{h \in \mathcal{A} \mid h\,\mathrm{k}\langle A\rangle \subseteq \mathrm{k}\langle A\rangle\} \quad \text{and} \quad \mathcal{H}_r(A) := \{h \in \mathcal{A} \mid \mathrm{k}\langle A\rangle\, h \subseteq \mathrm{k}\langle A\rangle\}$$

for the left and right stabilizers of $\mathrm{k}\langle A\rangle$ in $\mathcal{A}$. Clearly $\mathcal{H}_l(A)$ and $\mathcal{H}_r(A)$ are subalgebras. In particular, when $\mathcal{A}$ is commutative, $\mathcal{H}_l(A) = \mathcal{H}_r(A)$ is a commutative k-algebra that we simply write $\mathcal{H}(A)$. If $\mathcal{H}_l(A)$ (resp. $\mathcal{H}_r(A)$) is not equal to k, we say that $\mathrm{k}\langle A\rangle$ is *left periodic* (resp. *right periodic*). Observe also that for A and B two finite subsets of $\mathcal{A}$, if $\mathrm{k}\langle A\rangle$ is left periodic (resp. $\mathrm{k}\langle B\rangle$ is right periodic), then $\mathrm{k}\langle AB\rangle$ is left periodic (resp. right periodic). Indeed, for $\mathrm{k}\langle A\rangle$ left periodic, we have $\mathcal{H}_l(A) \neq \mathrm{k}$ and $\mathcal{H}_l(A)\mathrm{k}\langle A\rangle \subseteq \mathrm{k}\langle A\rangle$. By linearity of the multiplication in $\mathcal{A}$, this gives $\mathcal{H}_l(A)\mathrm{k}\langle AB\rangle \subseteq \mathrm{k}\langle AB\rangle$ thus $\mathcal{H}_l(A) \subseteq \mathcal{H}_l(AB)$ and $\mathcal{H}_l(AB) \neq \mathrm{k}$. The case $\mathrm{k}\langle B\rangle$ right periodic is similar.

Remark 2.2. The stabilizer algebra $\mathcal{H}_l(A)$ (resp. $\mathcal{H}_r(A)$) may also be described as the biggest subalgebra of $\mathcal{A}$ such that $\mathrm{k}\langle A\rangle$ is a left (resp. right) representation for this subalgebra.

Assume A is a finite subset of $\mathcal{A}_*$ such that $A \cap U(\mathcal{A}) \neq 0$. Then $\mathcal{H}_l(A)$ and $\mathcal{H}_r(A)$ are finite-dimensional k-subalgebras of $\mathcal{A}$. Indeed, for any $a \in A \cap U(\mathcal{A})$, we have $\mathcal{H}_l(A)a \subset \mathrm{k}\langle A\rangle$ and $a\mathcal{H}_r(A) \subset \mathrm{k}\langle A\rangle$ with

$$\dim_{\mathrm{k}}(\mathcal{H}_l(A)a) = \dim_{\mathrm{k}}(\mathcal{H}_l(A)) \quad \text{and} \quad \dim_{\mathrm{k}}(a\mathcal{H}_r(A)) = \dim_{\mathrm{k}}(\mathcal{H}_r(A)).$$

For any subset A in $\mathcal{A}_*$, we define

$$\mathrm{ann}_l(A) := \{a \in \mathcal{A} \mid a\,\mathrm{k}\langle A\rangle = \{0\}\} \quad \text{and} \quad \mathrm{ann}_r(A) := \{a \in \mathcal{A} \mid \mathrm{k}\langle A\rangle\, a = \{0\}\}$$

for the left and right annihilator of $\mathrm{k}\langle A\rangle$ in $\mathcal{A}$. Observe $\mathrm{ann}_l(A)$ and $\mathrm{ann}_r(A)$ are not subalgebras of $\mathcal{A}$ since they do not contain 1 but respectively a left ideal and a right ideal of $\mathcal{A}$. Moreover $\mathrm{ann}_l(A)$ (resp. $\mathrm{ann}_r(A)$) is a two-sided ideal of $\mathcal{H}_l(A)$ (resp. $\mathcal{H}_r(A)$) and $\mathrm{k} \oplus \mathrm{ann}_l(A)$ and $\mathrm{k} \oplus \mathrm{ann}_r(A)$ are respectively subalgebras of $\mathcal{H}_l(A)$ and $\mathcal{H}_r(A)$.

When $\mathcal{A}$ is commutative, we write $\mathrm{ann}_l(A) = \mathrm{ann}_r(A) = \mathrm{ann}(A)$. Also when $A = \{x_1, \dots, x_r\}$ is finite, we have

$$\mathrm{ann}_l(A) = \bigcap_{i=1}^{r} \mathrm{ann}_l(x_i).$$

2.2. **Basis of invertible elements.** Let $\mathcal{A}$ be an algebra over the field k. The algebra $\mathcal{A}$ has no non trivial finite-dimensional subalgebra when for any a in $\mathcal{A} \setminus k$, the algebra morphism

$$\theta_a : \begin{cases} \mathrm{k}[T] \to \mathcal{A} \\ P \longmapsto P(a) \end{cases}$$

is injective. This means that $\mathrm{k}[a] = \mathrm{Im}\,\theta_a$ is isomorphic to $\mathrm{k}[T]$.

When $\mathcal{A}$ is finite-dimensional, for any element $a \in \mathcal{A}$, the k-subalgebra $\mathrm{k}[a]$ generated by a is isomorphic to $\mathrm{k}[T]/(\mu_a)$ where μ_a is the minimal polynomial of a and $\ker\theta_a = (\mu_a)$. In particular, $\mathrm{k}[a]$ is a field if and only if μ_a is irreducible over k.

Lemma 2.3. *Assume $\mathcal{A}$ is finite-dimensional and consider $a \in A$ such that $a \notin U(\mathcal{A})$. Then, there exists $P \in \mathrm{k}[T]$ such that $aP(a) = 0$ and $P(a) \neq 0$.*

Proof. Since $a \notin U(\mathcal{A})$, the minimal polynomial μ_a is divisible by T. Let us write $\mu_a = TP(T)$ with $P(T) \in k[T]$. We have $P(a) \neq 0$ since $\deg P < \deg \mu_a$ and $aP(a) = \mu_a(a) = 0$. □

Recall the algebras we shall consider are unital and associative over the infinite field k. In addition we will restrict ourself most of the time to finite-dimensional algebras, Banach algebras over $\mathrm{k} = \mathbb{R}$ or $\mathrm{k} = \mathbb{C}$ or finite product of field extensions over k. In the case of Banach algebras, we will write $\|\cdot\|$ for the ambient norm.

Lemma 2.4. *Assume $\mathcal{A}$ is a Banach algebra and consider a in $\mathcal{A}$ such that $\|a\| < 1$. Then $1 - a \in U(\mathcal{A})$.*

Proof. Since $\|a\| < 1$ and $\mathcal{A}$ is a complete space, we have

$$(1-a)^{-1} = \sum_{k=0}^{+\infty} a^k$$

□

Lemma 2.5. *Assume the algebra $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{s}}$ and consider $a \in \mathcal{A}$. There exist infinitely many $\lambda \in \mathrm{k}$ such that the elements of the form $a - \lambda 1$ belong to $U(\mathcal{A})$.*

Proof. Assume first that $\mathcal{A}$ is finite-dimensional. Let λ such that $a - \lambda 1$ is not invertible. By Lemma 2.3, there exists $P \in \mathrm{k}[T]$ such that $(a - \lambda 1)P(a - \lambda 1) = 0$ and $P(a - \lambda 1) \neq 0$. Set $Q(T) = P(T - \lambda)$. We then get, $(a - \lambda 1)Q(a) = 0$ and $Q(a) \neq 0$. This can be rewritten $aQ(a) = \lambda Q(a)$ with $Q(a) \neq 0$. Therefore $Q(a)$ is an eigenvector associated to the eigenvalue λ for the linear map $\varphi_a : \mathcal{A} \to \mathcal{A}$ defined by $\varphi_a(x) = ax$ for any $x \in \mathcal{A}$. Since $\mathcal{A}$ is finite-dimensional, the linear map φ can only admit a finite number of eigenvalues and we are done.

Now assume $\mathcal{A}$ is a Banach algebra. For any $|\lambda| > \|a\|$, Lemma 2.4 shows that $1 - \lambda^{-1}a \in U(A)$. Hence $-\lambda(1 - \lambda^{-1}a) = a - \lambda 1 \in U(A)$.

Let us now consider the third case: assume that $\mathcal{A} = K_1 \times \cdots \times K_m$ is a product of field extensions over k. Let $a = (a_1, \ldots, a_m) \in \mathcal{A}$ and choose $\lambda \in \mathrm{k}$ distinct from $a_1, \ldots, a_m$. □

Proposition 2.6. *Assume $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{s}}$ and let A be a finite subset in $\mathcal{A}$ such that $A \cap U(\mathcal{A}) \neq \emptyset$. Then the* k*-subspace $\mathrm{k}\langle A\rangle$ admits a basis of invertible elements.*

Proof. Let $a \in A \cap U(\mathcal{A})$. By replacing A by $a^{-1}A$, we can assume that $1 \in A$. The k-subspace $\mathrm{k}\langle A\rangle$ admits a basis containing 1 of the form $B = \{1, b_2, \ldots b_d\}$ with $d = \dim_{\mathrm{k}} A$. By using the previous lemma, there exits $\lambda_i \in \mathrm{k}$ such that each $b_i - \lambda_i 1$ is invertible. Then $B' = \{1, b_2 - \lambda_1 1, \ldots, b_d - \lambda_d 1\}$ is a k-basis of $\mathrm{k}\langle A\rangle$ containing only invertible elements. □

Lemma 2.7. *Assume $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{s}}$. Let V be a n-dimensional subspace of $\mathcal{A}$ such that $V \cap U(\mathcal{A}) \neq \emptyset$. Consider $\{x_1, \ldots, x_n\}$ a basis of V over* k *with x_1 invertible. Then*

1. *Any n vectors in the set*
$$X = \{x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n \mid \alpha \in \mathrm{k}\}$$
form a basis of V over k.
2. *The set X contains an infinite number of invertible elements, that is an infinite number of elements of the form $x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n, \alpha \in \mathrm{k}$ are invertible.*
3. *The set X contains a basis of V over* k *of invertible elements.*

Proof. Assertion 1 is an application of the Vandermonde determinant.

For assertion 2, assume first $\mathcal{A}$ is finite-dimensional. For any $\alpha \in \mathrm{k}$, set $x_\alpha = x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n$. Let $\varphi_\alpha : \mathcal{A} \to \mathcal{A}$ be the left multiplication by x_α in $\mathcal{A}$. Clearly x_α is invertible if and only if the linear map φ_α is an isomorphism of k-spaces. Write $P(\alpha) = \det \varphi_\alpha$ for the

determinant of the linear map φ_α. Then $P(\alpha)$ is a non zero polynomial in α since $P(0) \neq 0$. So $P(\alpha) = 0$ only for a finite number of $\alpha \in \mathrm{k}$ and we are done.

Now assume that $\mathcal{A}$ is a Banach algebra. Observe that x_a is invertible if and only if $y_\alpha = x_1^{-1}x_\alpha$ is. We have $y_\alpha = 1 + \alpha x_1^{-1}x_2 + \cdots + \alpha^{n-1}x_1^{-1}x_n$. Assume $|\alpha| \leq 1$. We get

$$\|1 - y_\alpha\| = \left\|\alpha x_1^{-1}x_2 + \cdots + \alpha^{n-1}x_1^{-1}x_n\right\| \leq |\alpha| \left(\left\|x_1^{-1}x_2\right\| + \cdots + \left\|x_1^{-1}x_n\right\|\right).$$

Therefore $\|1 - y_\alpha\| < 1$ for any α such that $|\alpha| < \left(\left\|x_1^{-1}x_2\right\| + \cdots + \left\|x_1^{-1}x_n\right\|\right)^{-1}$. By using Lemma 2.4 we obtain our assertion 2 for Banach algebras since there is infinitely many such α in $\mathbb{R}$ and $\mathbb{C}$.

Let us consider the third case: $\mathcal{A} = K_1 \times \cdots \times K_m$ is a product of field extensions over k. We write $x_i = (a_{i1}, \ldots, a_{im})$ for $i \in \{1, \ldots, n\}$. Then $x_1 + \alpha x_2 + \cdots + \alpha^{n-1}x_n$ is invertible if and only if for every $j \in \{1, \ldots, m\}$, $P_j(\alpha) := a_{1j} + \alpha a_{2j} + \cdots + \alpha^{n-1}a_{nj} \neq 0$. But $P_j \in K_j[X]$ is a non zero polynomial (since $a_{1j} \neq 0$) and hence has only a finite number of roots in the (commutative) field K_j and thus also in k.

Assertion 3 is a consequence of Assertions 1 and 2. □

3. Algebras with finitely many subalgebras

We resume the notation and the hypotheses of the previous section on the algebra $\mathcal{A}$. The goal of this section is to classify the finite-dimensional algebras with finitely many subalgebras. Such algebras will indeed appear in the Kneser type theorem we shall state in Section 4.

3.1. **Primitive element.** The first step of our classification is to show that a finite-dimensional algebras with finitely many subalgebras is generated by one element.

Lemma 3.1 (Union of subspaces)**.** *Let V be a finite-dimensional vector space over* k *and $V_1, \ldots, V_n$ proper subspaces of V. Then*

$$\bigcup_{i=1}^{n} V_i \subsetneq V$$

Proof. Since V_i is a proper subspace of V, it can be embedded in a hyperplane H_i of V which is the kernel of a linear form $\varphi_i \in V^* \setminus \{0\}$. Since the ring of polynomial functions on V is an integral domain (k is infinite), then

$$f = \prod_{i=1}^{n} \varphi_i$$

is a non zero function. Any vector $v \in V$ such that $f(v) \neq 0$ is not in the union of the V_i. □

Corollary 3.2. *Let $\mathcal{A}$ be a finite-dimensional algebra over* k *such that $\mathcal{A}$ has only a finite number of subalgebras. Then there exists $x \in \mathcal{A}$ such that $\mathcal{A} = \mathrm{k}[x]$. In particular, $\mathcal{A}$ is commutative and generated by only one element.*

Proof. Lemma 3.1 ensures us that there exists $x \in \mathcal{A}$ which is not in any proper subalgebra of $\mathcal{A}$. We then get $\mathcal{A} = \mathrm{k}[x]$. □

3.2. **Structure of finite-dimensional algebras with finitely many subalgebras.** The rest of this section is devoted to the study of algebras with only a finite number of subalgebras. Our aim is to prove a classification theorem for this kind of algebras (Theorem 3.12). The proof is divided in two steps. In the first step, we reduce through various easy lemmas the form for algebras with finite number of subalgebras. The second step shows that algebras of the form obtained in the first step has indeed a finite number of subalgebras.

Let us start our first step. Corollary 3.2 says that we can restrict our attention to algebras of the form $\mathrm{k}[T]/(P)$. We begin with an easy remark which will be very useful.

Remark 3.3. (Quotient – Subalgebra) If $\mathcal{A}$ is a finite-dimensional algebra over k such that $\mathcal{A}$ has only a finite number of subalgebras. Then every subalgebra or quotient $\mathcal{B}$ of $\mathcal{A}$ verifies the same property. This is obvious for subalgebras. For the quotient case, the subalgebras of $\mathcal{B}$ are in bijection with the subalgebras of $\mathcal{A}$ containing the kernel of the surjective map from $\mathcal{A}$ to $\mathcal{B}$.

Let us now construct finite-dimensional algebras with an infinite number of subalgebras.

Lemma 3.4. *For $n \geq 4$, $\mathrm{k}[T]/T^n$ has an infinite number of subalgebras.*

Proof. Due to the remark 3.3, it suffices to study the case $n = 4$. In this case, for $\lambda \neq \mu \in \mathrm{k}$, the subalgebras $\mathcal{A}_\lambda = \mathrm{k}[T^2 + \lambda T^3]$ and $\mathcal{A}_\mu = \mathrm{k}[T^2 + \mu T^3]$ are distinct subalgebras. Indeed, they are two dimensional algebras isomorphic to $\mathrm{k}[T]/T^2$. So $(1, T^2 + \lambda T^3)$ is a basis for $\mathcal{A}_\lambda$ and $T^2 + \mu T^3$ can not be written as a linear combination of 1 and $T^2 + \lambda T^3$ in $\mathrm{k}[T]/T^4$. For if evaluating at $T = 0$, $T^2 + \lambda T^3$ and $T^2 + \mu T^3$ would be colinear. □

Lemma 3.5. *For $n \geq 4$ and $P \in \mathrm{k}[T]$ a non constant polynomial, $\mathrm{k}[T]/P^n$ has an infinite number of subalgebras.*

Proof. Indeed, the subalgebra generated by P is isomorphic to $\mathrm{k}[T]/T^n$. So Remark 3.3 and Lemma 3.4 give the result. □

Lemma 3.6. *For $n = 2, 3$ and $P \in \mathrm{k}[T]$ with $\deg P \geq 2$ then $\mathrm{k}[T]/P^n$ has an infinite number of subalgebras.*

Proof. Thanks to remark 3.3, it suffices to consider the case $n = 2$. For $\lambda \in \mathrm{k}$, let us consider $Q_\lambda = (1 + \lambda T)P \in \mathrm{k}[T]/P^2$. The subalgebra $\mathcal{A}_\lambda$ of $\mathrm{k}[T]/P^2$ generated by Q_λ is isomorphic to $\mathrm{k}[T]/T^2$ and so is two dimensional. For $\lambda \neq \mu$, we have $\mathcal{A}_\lambda \neq \mathcal{A}_\mu$. Indeed, if $(1 + \mu T)P = \alpha + \beta(1 + \lambda T)P$ in $\mathrm{k}[T]/P^2$. Then, going into $\mathrm{k}[T]/P$, we get $\alpha = 0$ and so $P \mid (1 + \mu T) - \beta(1 + \lambda T)$. Since $\deg P \geq 2$, we obtain $(1 + \mu T) = \beta(1 + \lambda T)$, which is absurd. □

Lemma 3.7. *For $n, m \in \{2, 3\}$, $\mathrm{k}[T]/T^n \times \mathrm{k}[T]/T^m$ has an infinite number of subalgebras.*

Proof. Thanks to remark 3.3, it suffices to consider the case $m = n = 2$. For $\lambda \in \mathrm{k}$, the element $(T, \lambda T)$ generates an algebra isomorphic to $\mathrm{k}[T]/T^2$ denoted by $\mathcal{A}_\lambda$. For $\lambda \neq \mu$, we have $\mathcal{A}_\lambda \neq \mathcal{A}_\mu$. Indeed, if $(T, \mu T) = \alpha(1, 1) + \beta(T, \lambda T)$. Then, mapping T to 0, we get $\alpha = 0$ and $(T, \mu T)$ and $(T, \lambda T)$ are colinear which is not the case. □

Corollary 3.8. *Let $\mathcal{A}$ be a finite-dimensional algebra over k such that $\mathcal{A}$ has only a finite number of subalgebras. Then, there exist finite algebraic extensions of k, $L_1, \ldots, L_n$ generated over k by one element and two integers $\delta \in \{0, 1\}$ and $m \in \{2, 3\}$ such that.*

$$\mathcal{A} \overset{k\text{-}alg.}{\simeq} L_1 \times \cdots \times L_n \times (\mathrm{k}[T]/T^m)^\delta$$

Proof. Thanks to Corollary 3.2, we get $\mathcal{A} = \mathrm{k}[T]/P$. Let us write the irreducible decomposition of P

$$P = \prod_{i=1}^{s} P_i^{n_i}$$

with $P_i \in \mathrm{k}[T]$ irreducible, $n_i > 0$ and P_i and P_j non associated for $i \neq j$. Chinese Reminder theorem tells us that

$$\mathcal{A} \overset{k\text{-alg.}}{\simeq} \mathrm{k}[T]/{P_1}^{n_1} \times \cdots \times \mathrm{k}[T]/{P_s}^{n_s}.$$

In particular, $\mathrm{k}[T]/P_i^{n_i}$ is a quotient of $\mathcal{A}$.

So Remark 3.3 and Lemma 3.6 ensures us that $n_i = 1$ if $\deg P_i \geq 2$. In this case $L_i = \mathrm{k}[T]/P_i$ is a finite extension of k generated by one element.

If $\deg P_i = 1$, then $P_i = T - \lambda$ for some $\lambda \in \mathrm{k}$ and $\mathrm{k}[T]/P_i^{n_i}$ is isomorphic to $\mathrm{k}[T]/T^{n_i}$. Lemma 3.4 ensures us that $n_i \in \{1, 2, 3\}$. If $n_i = 1$ then we get k. Let us consider the case where $n_i \in \{2, 3\}$. Lemma 3.7 tells us that there is at most one factor of this type and we get the structure result. □

We have just shown that algebras with a finite number of subalgebras have a certain form (a finite product of fields generated by one element with possibly a $k[T]/T^2$ or $k[T]/T^3$ factor). Our aim is now to show that algebras with this given form have only a finite number of subalgebras. To prove this, we first show that we can restrict our attention to subalgebras generated by one element (Lemma 3.9) and then give a description of all the subalgebras generated by one element of such an algebra (Proposition 3.10).

Lemma 3.9 (Subalgebra generated by one element)**.** *Let $\mathcal{A}$ be a finite-dimensional algebra over* k*. Then $\mathcal{A}$ has only a finite number of subalgebras if and only if $\mathcal{A}$ has only a finite number of subalgebras generated by one element.*

Proof. The part only if is clear. Let us suppose that $\mathcal{A}$ has only a finite number of subalgebras generated by one element. Let $\mathcal{B}$ be a subalgebra of $\mathcal{A}$. We have $\mathcal{B} = \cup_{y\in\mathcal{B}}\mathrm{k}[y]$. So $\mathcal{B}$ is a union of subalgebras generated by one element. There is only a finite number of such subalgebras since there is only a finite number of subalgebras $\mathrm{k}[y]$. □

Let us now determine subalgebras generated by one element of algebras of the form $L_1 \times \cdots \times L_n \times \mathrm{k}[T]/T^m$ where $n, m \in \mathbb{N}$, L_i is an algebraic field extension of k.

Proposition 3.10. *Let $m, n \in \mathbb{N}$. For $i \in [\![1, m]\!]$, let L_i be an algebraic field extension of* k*. Set $\mathcal{A} = L_1 \times \cdots \times L_n \times \mathrm{k}[T]/T^m$. For simplicity write L_{n+1} for $\mathrm{k}[T]/T^m$ and for any $i \in [\![1, n+1]\!]$, let $p_i : \mathcal{A} \to L_i$ be the projection on the i^{th} factor.*

Let $\mathcal{B}$ be a subalgebra of $\mathcal{A}$ generated by one element and for $i \in [\![1, n+1]\!]$, $K_i = p_i(\mathcal{B}) \subset L_i$. There exists

(i) a partition of $[\![1, n+1]\!]$

$$[\![1\,,\, n+1]\!] = I_1 \bigsqcup \cdots \bigsqcup I_r$$

with $n+1 \in I_r$ if $m \neq 0$.

(ii) a family of integers $(i_1, \ldots, i_r) \in I_1 \times \cdots \times I_r$ with $i_r = n+1$ if $m \neq 0$. For every $j \in [\![1\,,\, r]\!]$, let us write $I_j = \{i_j, u_{j,1}, \ldots, u_{j,s_j}\}$.

(iii) For every $j \in [\![1\,,\, r]\!]$ and every $\ell \in [\![1\,,\, s_j]\!]$, k-algebras morphisms $\sigma_{j,\ell} : K_{i_j} \to K_{u_{j,\ell}}$

such that after reordering the factors of the product, we have

$$\mathcal{B}=\{(x_1,\sigma_{1,1}(x_1),\ldots,\sigma_{1,s_1}(x_1),x_2,\ldots,\sigma_{2,s_2}(x_2),\ldots,x_r,\ldots,\sigma_{r,s_r}(x_r)),\quad x_j\in K_{i_j}\ \text{for } j\in[\![1\,,\,r]\!]\}\,.$$

Proof. Let us start by giving an overview of the proof. Let $y \in \mathcal{A}$ such that $\mathcal{B} = \mathrm{k}[y]$. We write $y = (y_1, \ldots, y_{n+1})$ with $y_i \in L_i$ for all i. The partition we are looking for is in fact given by gathering together the y_i with the same minimal polynomial (except for y_{n+1} which may play a special role). After this, we link y_i and y_j with the same minimal polynomial through a morphism of algebras. We finally get the independence of blocks with different minimal polynomial using the Chinese remainder theorem.

Let us now begin the proof. We have $\mathrm{k}[y] = \{(Q(y_1), \ldots, Q(y_{n+1})),\ Q \in \mathrm{k}[T]\}$ and then $K_i = \mathrm{k}[y_i]$. We define the equivalence relation $\sim$ on $[\![1\,,\, n]\!]$ by $i \sim j$ if y_i and y_j have the same

minimal polynomial over k. This defines a partition of $[1\,,\,n] = J_1 \sqcup \cdots \sqcup J_s$. Let us now consider the index $n+1$. For $i = n+1$ (if $m \neq 0$), the minimal polynomial of y_{n+1} is of the form $(T-\lambda)^s$ for some $\lambda \in \mathrm{k}$ and $s \leq m$. If there exists $i \in [1\,,\,n]$ such that $y_i = \lambda \in \mathrm{k}$ then we add $n+1$ to the equivalence class of i and obtain a partition of $[1\,,\,n]$ in s parts. In this case, we set $r = s$ and we number these parts such that $n+1$ is in the part indexed by r. If there does not exist an i such that $y_i = \lambda$, then we set $r = s+1$ and add the part $\{n+1\}$ to the partition of $[1\,,\,n]$ to get the desired partition of $[1\,,\,n+1]$.

Finally, we write the partition of $[1\,,\,n+1]$ we just obtain:

$$[1\,,\,n+1] = I_1 \bigsqcup \cdots \bigsqcup I_r$$

For each part of the partition, we choose a representative i_j of the subset. If $n+1$ is not alone in his part, then we choose $n+1$ to be the representative of this subset.

First, assume that $m = 0$. For $j \in [1\,,\,r]$ and $\alpha \in I_j$ the elements y_α and y_{i_j} have the same minimal polynomial so there exists an isomorphism σ of extensions from $\mathrm{k}[y_{i_j}] = K_{i_j}$ to $\mathrm{k}[y_\alpha] = K_\alpha$ sending y_{i_j} to y_α. In particular, we have $\sigma(Q(y_{i_j})) = Q(y_\alpha)$ for all $Q \in \mathrm{k}[T]$.

To get the desired description of $\mathcal{B}$, it suffices now to find $Q_j \in \mathrm{k}[T]$ such that $Q_j(y_{i_j}) = 1$ and $Q_j(y_{i_\ell}) = 0$ for all $\ell \neq j$. This is possible since the minimal polynomial P_ℓ of the y_{i_ℓ} are prime to each other (they are irreducible and distinct): we write

$$1 = UP_j + V\prod_{\ell \neq j} P_\ell$$

and consider $Q_j = V\prod_{\ell \neq j} P_\ell$.

Let us now assume that $m \neq 0$. For $j \in [1\,,\,r-1]$, there is no difference with the preceding case. For $j = r$, we have to be more careful: for $\alpha \neq n+1 \in I_r$, we can define the following morphisms of algebras

$$K_{n+1} = \mathrm{k}[y_{n+1}] \overset{k\text{-alg.}}{\simeq} \mathrm{k}[T]/(T-\lambda)^s \to \mathrm{k}[T]/(T-\lambda) \overset{k\text{-alg.}}{\simeq} \mathrm{k} = K_\alpha$$

where the first isomorphism sends y_{n+1} to the class of T and the second isomorphism sends the class of T to $\lambda \in \mathrm{k} = K_\alpha$. So by composition, we get the desired morphism of algebras.

Finally, to get the desired description of $\mathcal{B}$ in this case, it suffices to adapt the Chinese remainder argument. For this, we remark that $(T-\lambda)^s$ is prime with every irreducible polynomial over k except $T-\lambda$. But the index $i \in [1\,,\,n]$ such that $T-\lambda$ is the minimal polynomial y_i are precisely in I_r. □

Corollary 3.11. *Let $L_1, \ldots, L_n$ be finite field extensions of* k *generated over* k *by one element. Consider also two integers $\delta \in \{0,1\}$ and $m \in \{2,3\}$. Then*

$$\mathcal{A} = L_1 \times \cdots \times L_n \times (\mathrm{k}[T]/T^m)^\delta$$

has only a finite number of subalgebras.

Proof. Lemma 3.9 shows that it suffices to prove that $\mathcal{A}$ has only a finite number of subalgebras generated by one element. But proposition 3.10 implies that a subalgebra of $\mathcal{A}$ generated by one element is determined by a family of subalgebras of the L_i and by algebra morphisms between them. But each L_i has only a finite number of subalgebras and moreover Dedekind Lemma ([1]) ensures us that there exists only a finite number of k-algebra morphisms with values in a finite extension of k. So there is only a finite number of such subalgebras. □

Finally we get the structure theorem for algebras with only a finite number of subalgebras.

Theorem 3.12. *Let $\mathcal{A}$ be a finite-dimensional algebra over* k*. Then the following statements are equivalent.*

(1) $\mathcal{A}$ *has only a finite number of subalgebras.*
(2) *There exists finite algebraic extensions* $L_1, \dots, L_n$ *generated over* k *by one element and two integers* $\delta \in \{0,1\}$ *and* $m \in \{2,3\}$ *such that*

$$\mathcal{A} \overset{k\text{-}alg.}{\simeq} L_1 \times \cdots \times L_n \times (\mathrm{k}[T]/T^m)^\delta. \tag{2}$$

(3) *There exists* $g \in \mathcal{A}$ *such that* $\mathcal{A} = \mathrm{k}[g]$ *where the minimal polynomial* μ_g *of* g *has the form*

$$\mu_g = P_1 \cdots P_n Q^{m\delta}$$

where $P_1, \dots, P_n, Q$ *are distinct irreducible polynomials in* $\mathrm{k}[T]$, $\delta \in \{0,1\}$, $m \in \{2,3\}$ *and* $\deg Q = 1$.

Proof. The theorem follows from Corollary 3.8 and Corollary 3.11. □

Remark 3.13. Consider an infinite-dimensional commutative algebra $\mathcal{A}$ with a finite number of finite-dimensional subalgebras $\mathcal{B}_1, \dots, \mathcal{B}_r$. There exist $g_1, \dots, g_r$ in $\mathcal{A}$ such that $\mathcal{B}_i = \mathrm{k}[g_i]$ for any $i = 1, \dots, r$. Then $\mathcal{B} = \mathrm{k}[g_1, \dots, g_r]$ is a finite-dimensional subalgebra of $\mathcal{A}$ containing the subalgebras $\mathcal{B}_1, \dots, \mathcal{B}_r$. Therefore $\mathcal{B}$ coincides in fact with one of the algebras $\mathcal{B}_i$. This means that all the finite-dimensional subalgebras of $\mathcal{A}$ appear as subalgebras of the finite-dimensional algebra $\mathcal{B} \subset \mathcal{A}$ and we have a structure theorem for $\mathcal{B}$.

Remark 3.14. Consider a k-algebra $\mathcal{A}$ with a finite number of subalgebras. Then $\mathcal{A}$ is finite-dimensional over k. Indeed, for $y \in \mathcal{A}$, $k[y]$ is finite-dimensional. Otherwise, $k[y]$ would be isomorphic to $k[T]$ and would have infinitely many subalgebras. Moreover, there are finitely many subalgebras of the form $k[y]$. Write these algebras $k[y_1], \dots, k[y_r]$. We then have

$$\mathcal{A} = \bigcup_{i=1}^{r} k[y_i] = \sum_{i=1}^{r} k[y_i]$$

since for each $y \in \mathcal{A}$, the algebra $k[y]$ coincides with one of the algebras $k[y_1], \dots, k[y_r]$. This equality shows that $\mathcal{A}$ is finite-dimensional.

3.3. **Some examples.**

3.3.1. *Algebras of functions defined on a finite set.* Let $S = \{s_1, \dots, s_n\}$ be a finite set and write $\mathcal{F}_S$ for the algebra of functions $f : S \to \mathrm{k}$. The algebra $\mathcal{F}_S$ is clearly isomorphic to k^n. Thus, applying Theorem 3.12 to $\mathcal{F}_S$ allows us to recover the very classical following fact : $\mathcal{F}_S$ admits a finite number of subalgebras parametrized by the partitions $S = \bigsqcup_{i=1}^{m} S_m$ of S. The subalgebra $\mathcal{F}_{S_1,\dots,S_m}$ associated to such a partition is the algebra of functions $f \in \mathcal{F}_S$ which are constant on each set $S_i, i = 1, \dots, m$. Observe also we have $\mathcal{F}_S = \mathrm{k}[f]$ for any function f such that $f(s_i) \neq f(s_j)$ for any $i \neq j$.

A special case is the algebra $\mathcal{F}_G$ of complex central functions defined on a group G. Here, S is the set of conjugacy classes of G. In particular the characters of G belongs to $\mathcal{F}_G$. Let us consider $A = \{\chi_0 = 1, \chi_1, \dots, \chi_r\}$ and $B = \{\varphi_0 = 1, \varphi_1, \dots, \varphi_s\}$ two subsets of irreducible characters corresponding to the irreducible representations $U_0 = \mathrm{k}, U_1, \dots, U_r$ and $V_0 = \mathrm{k}, V_1, \dots, V_s$, respectively. Recall that for any $(i,j) \in \{0, \dots, r\} \times \{0, \dots, s\}$, $\chi_i\varphi_j$ is the characters of the tensor product $U_i \otimes V_j$. Let $\mathcal{V}$ be the set of characters of the representations obtained as direct sums of some copies of the $U_i \otimes V_j$'s. Observe $\mathcal{V}$ is not a k-space since it only contains linear combinations of the $\chi_i\varphi_j$ with nonnegative integer coefficients. Nevertheless, we have $\mathrm{k}\langle\mathcal{V}\rangle = \mathrm{k}\langle AB\rangle$ since the family $\{\chi_i\varphi_j \mid (i,j) \in \{0, \dots, r\} \times \{0, \dots, s\}\}$ generates $\mathrm{k}\langle AB\rangle$ as a k-space. In particular, $\mathrm{k}\langle AB\rangle$ admits a basis of characters in $\mathcal{V}$. It follows that $\dim_{\mathrm{k}}(AB)$ is the maximal number of

linearly independent characters in $\mathcal{V}$. When G is abelian or the characters χ_i and φ_j are linear, $\dim_{\mathrm{k}}(AB)$ is simply the cardinality of $\{\chi_i\varphi_j \mid (i,j) \in \{0,\dots,r\}\times\{0,\dots,s\}\}$ since distinct linear characters are always independent.

3.3.2. *Matrix subalgebras with finitely many subalgebras.* It is easy to construct subalgebras of matrix algebras with the form (2). Indeed consider irreducible polynomials $P_1,\dots,P_n,Q$ and integers $m \in \{2,3\}$ and $\delta \in \{0,1\}$ as in Theorem 3.12 and their companion matrices $\mathcal{C}_{P_1},\dots,\mathcal{C}_{P_n},\mathcal{C}_{Q^m}$. Set

$$r = \deg(P_1) + \cdots + \deg(P_n) + m\delta\deg(Q)$$

and define M as the $r \times r$ matrix with coefficients in k obtained as the block diagonal matrix with blocs $\mathcal{C}_{P_1},\dots,\mathcal{C}_{P_n},\mathcal{C}_{Q^m}$ when $\delta = 1$ and $\mathcal{C}_{P_1},\dots,\mathcal{C}_{P_n}$ when $\delta = 0$. Then the subalgebra $\mathrm{k}[M]$ of $\mathcal{M}_r(\mathrm{k})$ has the form (2).

3.3.3. *Algebras of complex valued continuous functions on a connected space.* Consider I a connected space and define $\mathcal{C}_I$ as the $\mathbb{C}$-algebra of continuous functions $f : I \to \mathbb{C}$. Then, the unique finite-dimensional subalgebra of $\mathcal{C}_I$ is that of constant functions. Indeed if we consider $\mathcal{A}$ such a subalgebra and $f \in \mathcal{A}$, then the minimal polynomial μ_f is such that $\mu_f(f)(x) = 0$ for any $x \in I$. Hence all the values of the connected set $\operatorname{Im} f$ are zeroes for μ_f. Since the only finite connected sets of $\mathbb{C}$ are singletons, the set $\operatorname{Im} f$ is reduced to a point and f is constant.

4. Kneser type theorems

In this Section, we state an analogue of Kneser's theorem for algebras.

4.1. **Kneser-Diderrich theorem for a wide class of algebras.** In this section, $\mathcal{A}$ satisfies $\mathbf{H}_{\mathrm{s}}$ or $\mathbf{H}_{\mathrm{w}}$. Let us consider a finite nonempty subset A of $\mathcal{A}_*$. We say that A is commutative when $aa' = a'a$ for any $a, a' \in A$. This then implies that the elements of $\mathrm{k}\langle A\rangle$ are pairwise commutative. Moreover the algebra $\mathbb{A}(A)$ generated by A is then commutative. Typical examples of commutative sets are geometric progressions $A = \{a^r, a^{r+1},\dots,a^{r+s}\}$ with r and s integers. The following theorem is an analogue, for algebras, of a theorem by Diderrich [2] extending Kneser's theorem for arbitrary groups when only the subset A is assumed commutative.

Theorem 4.1. *Assume $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{w}}$ and consider A and B be two finite nonempty subsets of $\mathcal{A}_*$ such that $\mathrm{k}\langle A\rangle \cap U(\mathcal{A}) \neq \emptyset$ and $\mathrm{k}\langle B\rangle \cap U(\mathcal{A}) \neq \emptyset$. Assume that A is commutative and $\mathbb{A}(A)$ admits a finite number of finite-dimensional subalgebras. Let $\mathcal{H} := \mathcal{H}_l(AB)$.*

(1) *We have*

$$\dim_{\mathrm{k}}(AB) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B) - \dim(\mathcal{H})$$

In particular, if AB is not left periodic

$$\dim_{\mathrm{k}}(AB) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B) - 1$$

(2) *If $\mathcal{A}$ is commutative, then*

$$\dim_{\mathrm{k}}(AB) \geq \dim_{\mathrm{k}}(\mathcal{H}A) + \dim_{\mathrm{k}}(\mathcal{H}B) - \dim_{\mathrm{k}}(\mathcal{H}) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B) - \dim_{\mathrm{k}}(\mathcal{H})$$

To prove this theorem we need the following preparatory lemma.

Lemma 4.2. *Assume $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{s}}$. Let A and B be two finite subsets of $\mathcal{A}_*$ such that A is commutative, $\mathrm{k}\langle A\rangle \cap U(\mathcal{A}) \neq \emptyset$ and $\mathrm{k}\langle B\rangle \cap U(\mathcal{A}) \neq \emptyset$. Then, for each $a \in \mathrm{k}\langle A\rangle \cap U(\mathcal{A})$, there exists a (commutative) finite-dimensional subalgebra $\mathcal{A}_a$ of $\mathcal{A}$ such that $\mathrm{k} \subseteq \mathcal{A}_a \subseteq \mathbb{A}(A)$ and a vector space V_a contained in $\mathrm{k}\langle AB\rangle$ such that $V_a \cap U(\mathcal{A}) \neq \emptyset$, $\mathcal{A}_aV_a = V_a$, $\mathrm{k}\langle aB\rangle \subseteq V_a$ and*

$$\dim_{\mathrm{k}}(V_a) + \dim_{\mathrm{k}}(\mathcal{A}_a) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B).$$

Proof. The hypothesis on a $\mathcal{A}$ ensures that each subspace of $\mathcal{A}$ containing an invertible element admits a basis of invertible elements (see Proposition 2.6).

By replacing A by $A' = a^{-1}A$ with $a \in \mathrm{k}\langle A\rangle \cap U(\mathcal{A}) \neq \emptyset$, we can establish the lemma only for $a = 1$. Indeed, if there exist a subalgebra $\mathcal{B} \subseteq \mathbb{A}(A')$ and a vector space $V \neq \{0\}$ contained in $\mathrm{k}\langle A'B\rangle$ such that $\mathcal{B}V = V$ and $\mathrm{k}\langle B\rangle \subseteq V$ with

$$\dim_{\mathrm{k}}(V) + \dim_{\mathrm{k}}(\mathcal{B}) \geq \dim_{\mathrm{k}}(A') + \dim_{\mathrm{k}}(B),$$

it suffices to take $V_a = aV$ and $\mathcal{A}_a = \mathcal{B} \subseteq \mathbb{A}(A') \subseteq \mathbb{A}(A)$. Since $\mathcal{B} \subseteq \mathbb{A}(A)$, we must have $\mathcal{B}a = a\mathcal{B}$ for any $a \in A$ and $\mathcal{B}(V_a) = \mathcal{B}(aV) = a\mathcal{B}V = aV = V_a$. Moreover $\mathrm{k}\langle aB\rangle = a\mathrm{k}\langle B\rangle \subseteq aV = V_a$ and $\dim_{\mathrm{k}}(V_a) + \dim_{\mathrm{k}}(\mathcal{A}_a) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B)$ because $\dim_{\mathrm{k}}(V_a) = \dim_{\mathrm{k}}(V)$ and $\mathcal{A}_a = \mathcal{B}$.

We can also assume that $1 \in B$ by replacing B by $B' = Bb^{-1}$ with $b \in \mathrm{k}\langle B\rangle \cap U(\mathcal{A}) \neq \emptyset$. Indeed, if there exist a subalgebra $\mathcal{B}' \subseteq \mathbb{A}(A)$ and a vector space $V' \neq \{0\}$ contained in $\mathrm{k}\langle AB'\rangle$ such that $\mathcal{B}'V' = V'$ and $\mathrm{k}\langle B'\rangle \subseteq V'$ with

$$\dim_{\mathrm{k}}(V') + \dim_{\mathrm{k}}(\mathcal{B}') \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B'),$$

it suffices to take $V = V'b$ and $\mathcal{A}_a = \mathcal{B}'$. We will have then $V = V'b \subseteq \mathrm{k}\langle AB'\rangle b = \mathrm{k}\langle AB\rangle$, $\mathcal{A}_a V = \mathcal{B}'(V'b) = (\mathcal{B}'V')b = V'b = V$, $\mathrm{k}\langle B\rangle = \mathrm{k}\langle B'\rangle b \subseteq V'b = V$ and

$$\dim_{\mathrm{k}}(V) + \dim_{\mathrm{k}}(\mathcal{A}_a) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B)$$

since $\dim_{\mathrm{k}}(B) = \dim_{\mathrm{k}}(B')$ and $\dim_{\mathrm{k}}(V) = \dim_{\mathrm{k}}(V')$.

We thus assume in the remainder of the proof that $1 \in A \cap B$ and proceed by induction on $\dim_{\mathrm{k}}(A)$. When $\dim_{\mathrm{k}}(A) = 1$, we have $\mathrm{k}\langle A\rangle = \mathrm{k} = \mathbb{A}(A)$. It suffices to take $V_1 = V = \mathrm{k}\langle B\rangle$ (with $1 \in B$) and $\mathcal{A}_1 = \mathrm{k} = \mathbb{A}(A)$. Assume $\dim_{\mathrm{k}}(A) > 1$. Given $e \in \mathrm{k}\langle B\rangle \cap U(\mathcal{A})$, define $A(e)$ and $B(e)$ to be finite subsets of $\mathcal{A}_*$ such that

$$\mathrm{k}\langle A(e)\rangle = \mathrm{k}\langle A\rangle \cap \mathrm{k}\langle B\rangle e^{-1} \quad \text{and} \quad \mathrm{k}\langle B(e)\rangle = \mathrm{k}\langle B\rangle + \mathrm{k}\langle A\rangle e.$$

Observe that $\mathrm{k}\langle A(e)\rangle$ and $\mathrm{k}\langle B(e)\rangle$ contain k since $1 \in A \cap B$. Thus we may and do assume that $1 \in A(e) \cap B(e)$. Moreover, $\mathrm{k}\langle A(e)\rangle\mathrm{k}\langle B(e)\rangle$ is contained in $\mathrm{k}\langle AB\rangle$. Indeed, for $v \in \mathrm{k}\langle A\rangle \cap \mathrm{k}\langle B\rangle e^{-1}$ and $w \in \mathrm{k}\langle B\rangle$, we have $vw \in \mathrm{k}\langle A\rangle\mathrm{k}\langle B\rangle \subseteq \mathrm{k}\langle AB\rangle$ because $v \in \mathrm{k}\langle A\rangle$. Set $v = ze^{-1}$ with $z \in \mathrm{k}\langle B\rangle$. If $w \in \mathrm{k}\langle A\rangle e$, we have $vw \in ze^{-1}\mathrm{k}\langle A\rangle e$. But $ze^{-1} \in \mathrm{k}\langle A\rangle$ and A is commutative. Therefore, $vw \in \mathrm{k}\langle A\rangle ze^{-1}e = \mathrm{k}\langle A\rangle z \subseteq \mathrm{k}\langle A\rangle\mathrm{k}\langle B\rangle \subseteq \mathrm{k}\langle AB\rangle$. In particular, $\dim_{\mathrm{k}}(A(e)B(e)) \leq \dim_{\mathrm{k}}(AB)$. We get

$$\dim_{\mathrm{k}}(A(e)) + \dim_{\mathrm{k}}(B(e)) = \dim_{\mathrm{k}}(\mathrm{k}\langle A\rangle \cap \mathrm{k}\langle B\rangle e^{-1}) + \dim_{\mathrm{k}}(\mathrm{k}\langle B\rangle + \mathrm{k}\langle A\rangle e) =$$
$$\dim_{\mathrm{k}}(\mathrm{k}\langle A\rangle e \cap \mathrm{k}\langle B\rangle) + \dim_{\mathrm{k}}(\mathrm{k}\langle B\rangle + \mathrm{k}\langle A\rangle e) = \dim_{\mathrm{k}}(Ae) + \dim_{\mathrm{k}}(B) = \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B).$$

Also $A(e) \subseteq \mathrm{k}\langle A\rangle$.

Assume $\mathrm{k}\langle A(e)\rangle = \mathrm{k}\langle A\rangle$ for any $e \in \mathrm{k}\langle B\rangle \cap U(\mathcal{A})$. Then $\mathrm{k}\langle A\rangle e \subseteq \mathrm{k}\langle B\rangle$ for any $e \in \mathrm{k}\langle B\rangle \cap U(\mathcal{A})$. Thus $\mathrm{k}\langle AB\rangle \subseteq \mathrm{k}\langle B\rangle$ by Proposition 2.6. Indeed $\mathrm{k}\langle B\rangle$ admits a basis contained in $U(\mathcal{A})$ and the products xy with $x \in A$ and $y \in \mathrm{k}\langle B\rangle \cap U(\mathcal{A})$ generate $\mathrm{k}\langle AB\rangle$. Since $1 \in A$, we have in fact $\mathrm{k}\langle AB\rangle = \mathrm{k}\langle B\rangle$. The subalgebra $\mathcal{A}_1 = \mathbb{A}(A)$ is commutative. Take $V_1 = \mathrm{k}\langle B\rangle$ (with $1 \in B$). Then $\mathcal{A}_1 V_1 = V_1$ since $\mathrm{k}\langle AB\rangle \subseteq \mathrm{k}\langle B\rangle$. In particular, $\mathcal{A}_1$ is finite-dimensional since $1 \in V_1$. We clearly have $V_1 = \mathrm{k}\langle AB\rangle$ and $\mathrm{k}\langle B\rangle \subseteq \mathrm{k}\langle AB\rangle = V_1$ as desired. We also get

$$\dim_{\mathrm{k}}(V_1) + \dim_{\mathrm{k}}(\mathcal{A}_1) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B).$$

Now assume $\mathrm{k}\langle A(e)\rangle \neq \mathrm{k}\langle A\rangle$ for at least one $e \in \mathrm{k}\langle B\rangle \cap U(\mathcal{A})$. Then $0 < \dim_{\mathrm{k}}(A(e)) < \dim_{\mathrm{k}}(A)$ and $1 \in A(e) \cap B(e)$. By our induction hypothesis, there exists a finite-dimensional subalgebra $\mathcal{A}_1$ of $\mathbb{A}(A(e)) \subseteq \mathbb{A}(A)$ and a nonzero k-vector space $V_1 \subseteq \mathrm{k}\langle A(e)B(e)\rangle \subseteq \mathrm{k}\langle AB\rangle$, such that $V_1 \cap U(\mathcal{A}) \neq \emptyset$, $\mathcal{A}_1 V_1 = V_1$ and $\mathrm{k}\langle B\rangle \subseteq \mathrm{k}\langle B(e)\rangle \subseteq V_1$ with

$$\dim_{\mathrm{k}}(V_1) + \dim_{\mathrm{k}}(\mathcal{A}_1) \geq \dim_{\mathrm{k}}(A(e)) + \dim_{\mathrm{k}}(B(e)) = \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B).$$

The subalgebra $\mathcal{A}_1 \subseteq \mathbb{A}(A)$ and the nonzero space $V_1 \supset \mathrm{k}\langle B\rangle$ satisfy the statement of the lemma for the pair of subsets A and B which concludes the proof. □

We are now ready to prove 4.1.

Proof. (of Theorem 4.1)

We first remark that if $\mathcal{A}$ is a subalgebra of an algebra $\mathcal{B}$ then the stabilizer of $k\langle AB\rangle$ in $\mathcal{B}$ is the stabilizer of $k\langle AB\rangle$ in $\mathcal{A}$. Indeed, for $a \in A \cap U(\mathcal{A})$, $b \in B \cap U(\mathcal{A})$ and x in the stabilizer of $k\langle AB\rangle$ in $\mathcal{B}$, we have $xab \in k\langle AB\rangle$ and so $x \in k\langle AB\rangle b^{-1}a^{-1} \subset \mathcal{A}$.

Since A stays commutative in $\mathcal{B}$ and $\mathbb{A}(A) \subset \mathcal{A} \subset \mathcal{B}$ has also a finite number of finite dimensional subalgebras, it suffices to prove our theorem when $\mathcal{A}$ satisfies $\mathbf{H}_{\mathrm{s}}$.

1: Let $\{x_1, \dots, x_n\}$ be a basis of $\mathrm{k}\langle A\rangle$ with x_1 invertible. For any $\alpha \in \mathrm{k}$, set $x_\alpha = x_1 + \alpha x_2 + \cdots + \alpha^{n-1}x_n$. Assume x_α is invertible. Since k is infinite and by Lemma 4.2, there exists a finite-dimensional subalgebra $\mathcal{A}_\alpha$ such that $\mathrm{k} \subseteq \mathcal{A}_\alpha \subseteq \mathbb{A}(A) \subseteq \mathcal{A}$ and a k-vector space $V_\alpha \subseteq \mathrm{k}\langle AB\rangle$ with $x_\alpha B \subseteq V_\alpha$, $\mathcal{A}_\alpha V_\alpha = V_\alpha$, $V_\alpha \cap U(\mathcal{A}) \neq \emptyset$ and

$$\dim_{\mathrm{k}}(V_\alpha) + \dim_{\mathrm{k}}(\mathcal{A}_\alpha) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B). \tag{3}$$

Since $\mathcal{A}_\alpha \subseteq \mathbb{A}(A)$ and $\mathbb{A}(A)$ is commutative and admits a finite number of finite-dimensional subalgebras containing k, there should exist by Lemma 2.7 n distinct scalars $\alpha_1, \dots, \alpha_n$ in k such that

$$\mathcal{A}_{\alpha_1} = \mathcal{A}_{\alpha_2} = \cdots = \mathcal{A}_{\alpha_n} = \mathcal{B}$$

and $x_{\alpha_1}, \dots, x_{\alpha_n}$ form a basis of invertible elements of $\mathrm{k}\langle A\rangle$ over k. We thus have $\mathrm{k}\langle AB\rangle = \sum_{i=1}^n x_{\alpha_i}\mathrm{k}\langle B\rangle \subseteq \sum_{i=1}^n V_{\alpha_i}$ since $x_{\alpha_i}\mathrm{k}\langle B\rangle \subseteq V_{\alpha_i}$ for any $i = 1, \dots, n$. On the other hand, $V_{\alpha_i} \subseteq \mathrm{k}\langle AB\rangle$ for any $i = 1, \dots, n$. Hence $\mathrm{k}\langle AB\rangle = \sum_{i=1}^n V_{\alpha_i}$ and

$$\mathcal{B}\mathrm{k}\langle AB\rangle = \mathcal{B}\sum_{i=1}^n V_{\alpha_i} = \sum_{i=1}^n \mathcal{A}_{\alpha_i}V_{\alpha_i} = \sum_{i=1}^n V_{\alpha_i} = \mathrm{k}\langle AB\rangle.$$

So $\mathcal{B} \subset \mathcal{H}$. Moreover

$$\dim_{\mathrm{k}}(AB) + \dim_{\mathrm{k}}(\mathcal{H}) \geq \dim_{\mathrm{k}}(AB) + \dim_{\mathrm{k}}(\mathcal{B}) \geq \dim_{\mathrm{k}}(V_{\alpha_1}) + \dim_{\mathrm{k}}(\mathcal{A}_{\alpha_1}) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B)$$

by (3) and because $V_{\alpha_1} \subset \mathrm{k}\langle AB\rangle$.

2: The space $\langle \mathcal{H}A\rangle$ contains A and is finite-dimensional because both $\mathcal{H}$ and $\mathrm{k}\langle AB\rangle$ are. Similarly, $\langle \mathcal{H}B\rangle$ contains B and is finite-dimensional. Let A' and B' be finite sets such that $\langle \mathcal{H}A\rangle = \langle A'\rangle$, $\langle \mathcal{H}B\rangle = \langle B'\rangle$, $A \subset A'$ and $B \subset B'$. Observe first that

$$\langle A'B'\rangle = \langle \mathcal{H}A\mathcal{H}B\rangle = \langle \mathcal{H}AB\rangle = \langle AB\rangle$$

for $\mathcal{A}$ is commutative and $\langle \mathcal{H}AB\rangle = \langle AB\rangle$. We then get Assertion 2 applying Assertion 1 to A' and B'.

□

Corollary 4.3. *Let $\mathcal{A}$ be a commutative Banach algebra with no non trivial finite-dimensional subalgebra. Then for any finite subsets A and B such that $\mathrm{k}\langle A\rangle \cap U(\mathcal{A}) \neq \emptyset$ and $\mathrm{k}\langle B\rangle \cap U(\mathcal{A}) \neq \emptyset$, we have*

$$\dim_{\mathrm{k}}(AB) \geq \dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B) - 1.$$

Example 4.4. *The previous corollary applies in particular to the Banach algebra $\mathcal{A} = \mathcal{C}_0(I)$ where I is any compact interval in $\mathbb{R}$ (or more generally I is a compact and connected set) and $\mathcal{C}_0(I)$ is the set of continuous functions $f : I \to \mathbb{R}$.*

Remark 4.5. Assume A and B as in Theorem 4.1 and $\dim_{\mathrm{k}}(A) + \dim_{\mathrm{k}}(B) > \dim_{\mathrm{k}}(\mathcal{A})$. Then, for any invertible $x \in \mathcal{A}$, we get

$$\dim_{\mathrm{k}}(\mathrm{k}\langle AB\rangle \cap \mathcal{H}x) > 0.$$

If $\mathcal{H}$ is a field (which is the case when $\mathcal{A}$ is a field), this shows that $x \in \mathrm{k}\langle AB\rangle$ and we have in this case $\mathrm{k}\langle AB\rangle = \mathcal{A}$. In the general case, $\mathcal{H}$ is not a field and we can have $\mathrm{k}\langle AB\rangle \subsetneqq \mathcal{A}$. For example, consider $\mathcal{A} = \mathrm{k}^n$ with $n \geq 3$ and $A = B$ the subalgebra of vectors whose last two coordinates are equal. In this case, we have $AB = A = B$.

With Theorem 4.1 in hand, one can prove the following generalization to arbitrary finite Minkowski products. The proof is similar to that of Theorem 2.7 in [12] so we omit it.

Theorem 4.6. *Assume $\mathcal{A}$ is a commutative finite-dimensional algebra, a commutative subalgebra of a Banach algebra or a subalgebra of a product of field extensions over* k. *Assume $\mathcal{A}$ contains only a finite number of finite-dimensional subalgebras. Consider a collection of finite subsets $A_1, \dots, A_n$ of $\mathcal{A}^*$ such that $\mathrm{k}\langle A_i\rangle \cap U(\mathcal{A}) \neq \emptyset$ for any $i = 1, \dots, n$. Set $\mathcal{H} := \mathcal{H}(A_1 \cdots A_n)$. The following statements hold and are equivalent:*

1. $\dim_{\mathrm{k}}(A_1 \cdots A_n) \geq \sum_{i=1}^{n} \dim_{\mathrm{k}}(A_i\mathcal{H}) - (n-1)\dim_{\mathrm{k}}(\mathcal{H})$,
2. $\dim_{\mathrm{k}}(A_1 \cdots A_n) \geq \sum_{i=1}^{n} \dim_{\mathrm{k}}(A_i) - (n-1)\dim_{\mathrm{k}}(\mathcal{H})$,
3. *any one of the above two statements in the case $n = 2$.*

Remark 4.7. In [8], Hou shows that in the context of non separable extension of fields, a counterexample to Theorem 4.1 could only arise with $\dim A \geq 6$. Following the proof given in [8], we are able to show that if $\dim A \leq 4$, then no hypotheses on $\mathbb{A}(A)$ other than commutativity is needed to get Theorem 4.1.

4.2. **Remarks on Olson type Theorem.** It is known that Kneser's theorem does not hold for non abelian group. In [15], Olson gave a weaker version of Kneser's theorem for arbitrary groups. This Olson theorem admits a natural linearization for division rings [3]. It is tempting to look for a possible analogue in our algebras context. In fact, by using the Kemperman linear transform defined in [3] and arguments closed from those we have used to establish Theorem 4.1 one can prove the following analogue of Olson's theorem where no hypothesis on the commutativity of $\mathcal{A}$ neither on the number of its finite-dimensional subalgebras is required.

Theorem 4.8. *Let $\mathcal{A}$ be a unital associative algebra over* k *satisfying $\boldsymbol{H}_{\mathrm{s}}$. Consider V, W finite-dimensional* k*-vector spaces in $\mathcal{A}$ such that $V \cap U(\mathcal{A}) \neq \emptyset$ and $W \cap U(\mathcal{A}) \neq \emptyset$. Then one of the two following assertions holds*

1. *There exists a* k*-vector subspace N of $\mathrm{k}\langle VW\rangle$ such that*
   - $N \cap U(\mathcal{A}) = \emptyset$,
   - $\dim_{\mathrm{k}} \mathrm{k}\langle VW\rangle \geq \dim_{\mathrm{k}} V + \dim_{\mathrm{k}} W - \dim_{\mathrm{k}}(N)$.
2. *There exist a* k*-vector subspace S of $\mathrm{k}\langle VW\rangle$ and a subalgebra $\mathcal{H}$ of $\mathcal{A}$ such that*
   - $S \cap U(\mathcal{A}) \neq \emptyset$,
   - $\mathrm{k} \subset \mathcal{H} \subset \mathcal{A}$,
   - $\dim_{\mathrm{k}} \mathrm{k}\langle VW\rangle \geq \dim_{\mathrm{k}} S \geq \dim_{\mathrm{k}} V + \dim_{\mathrm{k}} W - \dim_{\mathrm{k}} \mathcal{H}$,
   - $\mathcal{H}S = S$ *or* $S\mathcal{H} = S$.

Assertion 2 looks indeed as a natural analogue of Olson's theorem for algebras. Also, when $\mathcal{A}$ is a division ring, we must have $N = \{0\}$ in assertion 1. This is unfortunately not the case in general. Moreover, for an algebra $\mathcal{A}$, one can have few constraints on the dimensions of the subspaces N such that $N \cap U(\mathcal{A}) = \emptyset$. This is notably the case of the matrix algebra $M_n(\mathbb{C})$ which admits subspaces N of any dimension less than $n^2 - n$ containing no invertible matrices

or the Banach algebra of continuous functions from $[0,1]$ to $\mathbb{R}$. So it eventually appears that this Olson type theorem for algebras yields only few information on the dimension of the space products $\mathrm{k}\langle VW\rangle$.

Now, if we assume that V is commutative, we obtain immediately the following corollary of Lemma 4.2.

Corollary 4.9. *Assume $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{s}}$[1] and consider V, W finite-dimensional* k*-vector spaces in $\mathcal{A}$ such that V is commutative, $V \cap U(\mathcal{A}) \neq \emptyset$ and $W \cap U(\mathcal{A}) \neq \emptyset$. Then there exist a* k*-vector subspace S of $\mathrm{k}\langle VW\rangle$ and a finite-dimensional subalgebra $\mathcal{H}$ of $\mathcal{A}$ such that*

- $S \cap U(\mathcal{A}) \neq \emptyset$,
- $\mathrm{k} \subset \mathcal{H} \subset \mathcal{A}$,
- $\dim_{\mathrm{k}} \mathrm{k}\langle VW\rangle \geq \dim_{\mathrm{k}} S \geq \dim_{\mathrm{k}} V + \dim_{\mathrm{k}} W - \dim_{\mathrm{k}} \mathcal{H}$,
- $\mathcal{H}S = S$.

Proof. Choose $a \in V \cap U(\mathcal{A})$. By Lemma 4.2, there exists a (commutative) finite-dimensional subalgebra $\mathcal{H}$ of $\mathcal{A}$ such that $\mathrm{k} \subseteq \mathcal{H} \subseteq \mathbb{A}(A)$ and a vector space S contained in $\mathrm{k}\langle VW\rangle$ such that $S \cap U(\mathcal{A}) \neq \emptyset$, $\mathcal{H}S = S$ and

$$\dim_{\mathrm{k}}(S) + \dim_{\mathrm{k}}(\mathcal{H}) \geq \dim_{\mathrm{k}}(V) + \dim_{\mathrm{k}}(W).$$

□

5. Hamidoune and Tao type results

In this section, we assume $\mathcal{A}$ satisfies $\mathbf{H}_{\mathrm{s}}$ so that every subspace of $\mathcal{A}$ containing an invertible element admits a basis of invertible elements (Proposition 2.6).

5.1. **Linear hamidoune's connectivity.** The notion of connectivity for a subset S of a group G was developed by Hamidoune in [7]. As suggested by Tao in [17], it is interesting to generalize Hamidoune's definition by introducing an additional parameter λ. The purpose of this paragraph is to adapt this notion of connectivity to our algebra context. Assume V is a finite-dimensional fixed k-subspace of $\mathcal{A}$ such that $V \cap U(\mathcal{A}) \neq \emptyset$ and λ is a real parameter. For any finite-dimensional k-subspace W of $\mathcal{A}$, we define

$$c(W) := \dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) - \lambda \dim_{\mathrm{k}}(W). \tag{4}$$

For any $x \in U(\mathcal{A})$, we have immediately that $c(xW) = c(W)$.

Lemma 5.1. *For any finite-dimensional subspaces W_1, W_2 and V of $\mathcal{A}$, we have*

$$c(W_1 + W_2) + c(W_1 \cap W_2) \leq c(W_1) + c(W_2).$$

Proof. We have

$$\dim_{\mathrm{k}}(W_1 + W_2) + \dim_{\mathrm{k}}(W_1 \cap W_2) = \dim_{\mathrm{k}}(W_1) + \dim_{\mathrm{k}}(W_2) \tag{5}$$

and

$$\dim_{\mathrm{k}}(\mathrm{k}\langle W_1V\rangle + \mathrm{k}\langle W_2V\rangle) + \dim_{\mathrm{k}}(\mathrm{k}\langle W_1V\rangle \cap \mathrm{k}\langle W_2V\rangle) = \dim_{\mathrm{k}}(W_1V) + \dim_{\mathrm{k}}(W_2V).$$

Observe that $\mathrm{k}\langle (W_1 + W_2)\cdot V\rangle = \mathrm{k}\langle W_1V\rangle + \mathrm{k}\langle W_2V\rangle$ and $\mathrm{k}\langle (W_1 \cap W_2)\cdot V\rangle \subseteq \mathrm{k}\langle W_1V\rangle \cap \mathrm{k}\langle W_2V\rangle$. This gives

$$\dim_{\mathrm{k}}(\mathrm{k}\langle (W_1 + W_2)\cdot V\rangle) + \dim_{\mathrm{k}}(\mathrm{k}\langle W_1 \cap W_2)\cdot V\rangle) \leq \dim_{\mathrm{k}}(\mathrm{k}\langle W_1V\rangle) + \dim_{\mathrm{k}}(\mathrm{k}\langle W_2V\rangle). \tag{6}$$

We then obtain the desired equality by subtracting from (6), λ copies of (5). □

[1] Observe there is no hypothesis on the number of subalgebras of $\mathcal{A}$ here.

Similarly to [7], we define the *connectivity* $\kappa = \kappa(V)$ as the infimum of $c(W)$ over all finite-dimensional k-subspaces of $\mathcal{A}$ such that $W \cap U(\mathcal{A}) \neq \emptyset$. A *fragment* of V is a finite-dimensional k-subspace of $\mathcal{A}$ which attains the infimum κ. An *atom* of V is a fragment of minimal dimension. Since $c(xW) = c(W)$ for any $x \in U(\mathcal{A})$, any left translate by an invertible of a fragment is a fragment and any left translate of an atom is an atom. Since $\dim_{\mathrm{k}}(WV) \geq \dim_{\mathrm{k}}(W)$ (because $V \cap U(\mathcal{A}) \neq \emptyset$), we have

$$c(W) \geq (1-\lambda)\dim_{\mathrm{k}}(W). \tag{7}$$

We observe that when $\lambda < 1$, $c(W)$ is always positive and takes a discrete set of values. Therefore, when $\lambda \leq 1$, there exists at least one fragment and at least one atom. *In the remainder of this paragraph we will assume that* $0 < \lambda \leq 1$. Let W_1 and W_2 be two fragments such that $W_1 \cap W_2$ intersects $U(\mathcal{A})$. By the previous lemma, we derive

$$c(W_1 + W_2) + c(W_1 \cap W_2) \leq c(W_1) + c(W_2) = 2\kappa.$$

Since $W_1 + W_2$ and $W_1 \cap W_2$ are finite-dimensional and intersects $U(\mathcal{A})$, we must have $c(W_1 + W_2) \geq \kappa$ and $c(W_1 \cap W_2) \geq \kappa$. Hence $c(W_1 + W_2) = c(W_1 \cap W_2) = \kappa$. This means that $W_1 + W_2$ and $W_1 \cap W_2$ are also fragments. If we assume now that W_1 and W_2 are atoms such that $W_1 \cap W_2$ intersects $U(\mathcal{A})$, we obtain that $W_1 = W_2$.

Proposition 5.2. *Assume $\mathcal{A}$ satisfies $\boldsymbol{H}_{\mathrm{s}}$ and V is a finite-dimensional fixed* k*-subspace of $\mathcal{A}$ such that $V \cap U(\mathcal{A}) \neq \emptyset$*

1. *There exists a unique atom $\mathcal{H}_\lambda$ containing* 1 *for V.*
2. *This atom is a subalgebra of $\mathcal{A}$ containing $\mathcal{H}_l(V)$.*
3. *Moreover the atoms of V which intersect $U(\mathcal{A})$ are the right $\mathcal{H}_\lambda$-modules $x\mathcal{H}_\lambda$ where x runs over $U(\mathcal{A})$.*
4. *For any finite-dimensional* k*-subspace W satisfying $W \cap U(\mathcal{A}) \neq \emptyset$, we have*

$$\dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) \geq \lambda \dim_{\mathrm{k}}(W) + \dim_{\mathrm{k}}(V) - \lambda \dim_{\mathrm{k}}(\mathcal{H}_\lambda)$$

Proof. Since there exists at least one atom and the left translate of any atom by any invertible is an atom, there exists one atom $\mathcal{H}$ containing 1. Now, this atom must be unique. Indeed, if $\mathcal{H}'$ is another atom containing 1, we have that $\mathcal{H} \cap \mathcal{H}'$ intersects $U(\mathcal{A})$. Hence, by the previous arguments $\mathcal{H} = \mathcal{H}'$. Now, for any $h \in \mathcal{H} \cap U(\mathcal{A})$, we have that $\mathcal{H} \cap h^{-1}\mathcal{H}$ contains 1. Since both $\mathcal{H}$ and $h^{-1}\mathcal{H}$ are atoms, we must have $h^{-1}\mathcal{H} = \mathcal{H}$ and $\mathcal{H} = h\mathcal{H}$. So $\mathcal{H}$ is stable under multiplication by any invertible of $\mathcal{H}$. By Proposition 2.6, $\mathcal{H}$ is then stable by multiplication. We then deduce that $\mathcal{H}$ is a subalgebra of $\mathcal{A}$ by Lemma 2.1. Moreover, if $x \in \mathcal{H}_l(V)$ and $x \notin \mathcal{H}$, then $(\mathcal{H} + kx)V = \mathcal{H}V$ and so $c(\mathcal{H} + kx) < c(\mathcal{H})$ since $\lambda > 0$ contradicting the definition of an atom. Finally, given any atom W of V intersecting $U(\mathcal{A})$, we must have $w^{-1}W = \mathcal{H}$ for any $w \in W \cap U(\mathcal{A})$ since $\mathcal{H}$ is the unique atom containing 1 and $w^{-1}\mathcal{H}$ is an atom containing 1.

Let us now prove (4). By definition of κ, we have $\kappa = c(\mathcal{H}_\lambda) \leq c(W)$. This gives

$$\dim_{\mathrm{k}}(\mathrm{k}\langle \mathcal{H}_\lambda V\rangle) - \lambda \dim_{\mathrm{k}}(\mathcal{H}_\lambda) \leq \dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) - \lambda \dim_{\mathrm{k}}(W).$$

We thus get

$$\dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) \geq \lambda \dim_{\mathrm{k}}(W) + \dim_{\mathrm{k}}(\mathcal{H}_\lambda V) - \lambda \dim_{\mathrm{k}}(\mathcal{H}_\lambda) \geq \lambda \dim_{\mathrm{k}}(W) + \dim_{\mathrm{k}}(V) - \lambda \dim_{\mathrm{k}}(\mathcal{H}_\lambda).$$

□

Remark 5.3.

1. Assume $\mathcal{A}$ has no non trivial f.d. subalgebra. Then we must have $\mathcal{H}_\lambda = \mathrm{k}$ for any $\lambda \leq 1$. So we obtain

$$\dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) \geq \lambda(\dim_{\mathrm{k}}(W) - 1) + \dim_{\mathrm{k}}(V) \text{ for any } \lambda \leq 1.$$

In particular, for $\lambda = 1$, this gives

$$\dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) \geq \dim_{\mathrm{k}}(W) + \dim_{\mathrm{k}}(V) - 1$$

which generalizes Corollary 4.3.

(2) If V and W are such that $\dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) < \dim_{\mathrm{k}}(W) + \dim_{\mathrm{k}}(V) - 1$, then the unique atom $\mathcal{H}_1$ for V containing 1 is a subalgebra of $\mathcal{A}$ of dimension at least 2.

(3) Contrary to Theorem 4.1 where the lower bound makes appear the stabilizer of $\mathrm{k}\langle WV\rangle$, the subalgebra $\mathcal{H}_\lambda$ in the previous corollary only depends on λ and V and is the same for each subspace W.

5.2. **Tao's theorem for algebras.** We say that $V = \mathrm{k}\langle A\rangle$, where A is a finite subset of $\mathcal{A}$, is a *space of small doubling*, when $\dim_{\mathrm{k}}(A^2) = O(\dim_{\mathrm{k}}(A))$. Simplest examples of spaces of small doubling are the spaces $V = \mathrm{k}\langle A\rangle$ containing 1 and such that $\dim_{\mathrm{k}}(A^2) = \dim_{\mathrm{k}}(A)$. Then by Lemma 2.1, V is a subalgebra containing k. In general, a space of small doubling $\mathrm{k}\langle A\rangle$ is not a subalgebra and neither a left nor right $\mathcal{H}$-module for a subalgebra $\mathrm{k} \subseteq \mathcal{H} \subseteq \mathcal{A}$. The following theorem, which is a linear version of Theorem 1.2 in [17], permits to study the spaces of small doubling in an algebra $\mathcal{A}$ satisfying $\mathbf{H}_{\mathrm{s}}$.

Theorem 5.4. *Consider finite-dimensional* k*-subspaces V and W of $\mathcal{A}$ (satisfying $\boldsymbol{H}_{\mathrm{s}}$) intersecting $U(\mathcal{A})$ such that* $\dim_{\mathrm{k}}(W) \geq \dim_{\mathrm{k}}(V)$ *and* $\dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) \leq (2-\varepsilon)\dim_{\mathrm{k}}(V)$ *for some real ε such that $0 < \varepsilon < 2$. Then, there exists a finite-dimensional subalgebra $\mathcal{H}$ such that* $\dim_{\mathrm{k}}(\mathcal{H}) \leq (\frac{2}{\varepsilon}-1)\dim_{\mathrm{k}}(V)$*, and V is contained in the left $\mathcal{H}$-module $\mathcal{H}V$ with* $\dim_{\mathrm{k}}(\mathcal{H}V) \leq (\frac{2}{\varepsilon}-1)\dim_{\mathrm{k}}(\mathcal{H})$.

Proof. We apply linear Hamidoune connectivity with $\lambda = 1-\frac{\varepsilon}{2}$. We have by (7) $c(S) \geq \frac{\varepsilon}{2}\dim_{\mathrm{k}}(S)$ for any k-subspace S. This can be rewritten as

$$\dim_{\mathrm{k}}(S) \leq \frac{2}{\varepsilon}c(S). \tag{8}$$

We also get

$$c(W) := \dim_{\mathrm{k}}(\mathrm{k}\langle WV\rangle) - (1-\frac{\varepsilon}{2})\dim_{\mathrm{k}}(W) \leq (2-\varepsilon)\dim_{\mathrm{k}}(V) - (1-\frac{\varepsilon}{2})\dim_{\mathrm{k}}(V) = (1-\frac{\varepsilon}{2})\dim_{\mathrm{k}}(V).$$

since $\dim_{\mathrm{k}}(WV) \leq (2-\varepsilon)\dim_{\mathrm{k}}(V)$ and $\dim_{\mathrm{k}}(W) \geq \dim_{\mathrm{k}}(V)$. By Proposition 5.2, the unique atom containing 1 is a subalgebra $\mathcal{H}$. By definition of an atom, we should have

$$\kappa = c(\mathcal{H}) \leq c(W) \leq (1 - \frac{\varepsilon}{2})\dim_{\mathrm{k}}(V).$$

We therefore obtain, by using (8) with $S = \mathcal{H}$, that

$$\dim_{\mathrm{k}}(\mathcal{H}) \leq \frac{2}{\varepsilon}c(\mathcal{H}) \leq \frac{2}{\varepsilon}c(W) \leq (\frac{2}{\varepsilon} - 1)\dim_{\mathrm{k}}(V).$$

By using that $c(\mathcal{H}) = \dim_{\mathrm{k}}(\mathcal{H}V) - (1 - \frac{\varepsilon}{2})\dim_{\mathrm{k}}(\mathcal{H})$ and the previous inequality $c(\mathcal{H}) \leq (1 - \frac{\varepsilon}{2})\dim_{\mathrm{k}}(V)$, we get

$$\dim_{\mathrm{k}}(\mathcal{H}V) \leq (1 - \frac{\varepsilon}{2})\dim_{\mathrm{k}}(V) + (1 - \frac{\varepsilon}{2})\dim_{\mathrm{k}}(\mathcal{H}). \tag{9}$$

We can also bound $\dim_{\mathrm{k}}(V)$ by $\dim_{\mathrm{k}}(\mathcal{H}V)$ in (9). This yields

$$\dim_{\mathrm{k}}(\mathcal{H}V) \leq (\frac{2}{\varepsilon} - 1)\dim_{\mathrm{k}}(\mathcal{H}). \tag{10}$$

□

Remark 5.5.

(1) When $\dim_{\mathrm{k}}(V^2) \leq (2-\varepsilon)\dim_{\mathrm{k}}(V)$, we can apply Theorem 5.4 with $V = W$ and obtain that $V \subset \mathcal{H}V$ with

$$\dim_{\mathrm{k}}(\mathcal{H}) \leq (\frac{2}{\varepsilon} - 1)\dim_{\mathrm{k}}(V) \quad \text{and} \quad \dim_{\mathrm{k}}(\mathcal{H}V) \leq (\frac{2}{\varepsilon} - 1)\dim_{\mathrm{k}}(\mathcal{H}).$$

(2) When $\mathcal{A}$ has no non trivial f.d.subalgebra and $\dim_{\mathrm{k}}(V^2) \leq (2-\varepsilon)\dim_{\mathrm{k}}(V)$, we have $\mathcal{H} = \mathrm{k}$. So

$$\frac{1}{\frac{2}{\varepsilon} - 1} \leq \dim_{\mathrm{k}}(V) \leq \frac{2}{\varepsilon} - 1.$$

6. Groups setting

6.1. **Recovering results in the group setting.** The aim of this paragraph is to explain how Theorem 4.1 permits to recover Diderrich's theorem for groups. The proof goes through three steps. First we turn the group $\mathbb{G}$ into the group algebra $\mathrm{k}[\mathbb{G}]$. Second, we link the stabilizer in $\mathbb{G}$ of the subset A with the stabilizer in $\mathrm{k}[\mathbb{G}]$ of the subspace $\mathrm{k}\langle A\rangle$. Third we choose a convenient field (the field $\mathbb{C}$ of complex numbers) so that the subalgebra generated by $\mathrm{k}\langle A\rangle$ has only a finite number of subalgebras.

Let us now detail these ideas. First, the group algebra $\mathrm{k}[\mathbb{G}]$ is the k-vector space with basis $\{e_g \mid g \in \mathbb{G}\}$ and multiplication defined by $e_g \cdot e_{g'} = e_{gg'}$ for any g, g' in $\mathbb{G}$. Given any nonempty set A in $\mathbb{G}$, we define its associated set in $\mathrm{k}[\mathbb{G}]$ as $\overline{A} = \{e_a \mid a \in A\}$. It is clear that A is a commutative set in $\mathbb{G}$ if and only if $\overline{A}$ is a commutative set in $\mathrm{k}[\mathbb{G}]$. In that case, the subalgebra $\mathbb{A}(\overline{A})$ is a finite-dimensional commutative algebra isomorphic to $\mathrm{k}[\mathbb{G}(A)]$ the group algebra of the subgroup $\mathbb{G}(A)$ of $\mathbb{G}$ generated by the elements of A. Moreover, write

$$H = \{h \in \mathbb{G} \mid hA = A\} \quad \text{and} \quad \mathcal{H}_l = \{x \in \mathrm{k}[\mathbb{G}] \mid x\overline{A} \subset \mathrm{k}\langle\overline{A}\rangle\}$$

for the left stabilizer of A in $\mathbb{G}$ and the left stabilizer of $\mathrm{k}\langle\overline{A}\rangle$ in $\mathrm{k}[\mathbb{G}]$, respectively.

Lemma 6.1. *We have $\mathcal{H}_l = \mathrm{k}\langle\overline{H}\rangle = \mathrm{k}[H]$ that is, $\mathcal{H}_l$ is the group algebra of the group H.*

Proof. The inclusion $\mathcal{H}_l \supset \mathrm{k}\langle\overline{H}\rangle$ is immediate. For the converse, observe first that for any $g \notin H$, there exists a_g in A such that $ga_g \notin A$. Consider $x = \sum_{g\in G} \lambda_g e_g$ in $\mathcal{H}_l$ (where the coefficients λ_g are all but a finite number equal to zero when $\mathbb{G}$ is infinite). Since $\mathcal{H}_l \supset \mathrm{k}\langle\overline{H}\rangle$, we may assume that $\lambda_g = 0$ for all $g \in H$ and write $x = \sum_{g\notin H} \lambda_g e_g$. Our aim is to show that $\lambda_g = 0$ for all $g \notin H$. For such a g, there exists $a \in A$ such that $ga \notin A$. Moreover, since $x \in \mathcal{H}_l$ and $a \in A$, we have $xe_a \in \mathrm{k}[\overline{A}]$. Finally, we get

$$\sum_{g'\in A} \mu_{g'} e_{g'} = xe_a = \sum_{g'\notin H} \lambda_{g'} e_{g'} e_a = \sum_{g'\notin H} \lambda_{g'} e_{g'a}$$

Since the family $\{e_{g'}, g' \in \mathbb{G}\}$ is a basis for $\mathrm{k}[\mathbb{G}]$, we get $\lambda_g = 0$ comparing the coefficient of e_{ga} in the left and right hand side of the previous equality. □

To obtain Diderrich's theorem for groups from Theorem 4.1 and Lemma 6.1, we have to find a field such that $\mathbb{A}(\overline{A}) = \mathrm{k}[\mathbb{G}(A)]$ admits a finite number of subalgebras containing 1 and $\mathrm{k}[\mathbb{G}]$ verifies $\mathbf{H}_{\mathrm{s}}$. These two points relies on the two following lemmas.

Lemma 6.2. *Let $\mathbb{G}$ be a finitely generated commutative group. Then*

$$\mathbb{C}[\mathbb{G}] \simeq \mathbb{C}[{X_1}^{\pm 1}, \ldots, {X_r}^{\pm 1}]^m$$

thus is a product of integral algebras and has a finite number of finite dimensional subalgebras.

Proof. This is standard representation theory. We may write $\mathbb{G} \simeq \mathbb{Z}^r \times \mathbb{G}'$ with $\mathbb{G}'$ a finite group of order m. We then have $\mathbb{C}[\mathbb{G}] \simeq \mathbb{C}[\mathbb{Z}^r] \otimes \mathbb{C}[\mathbb{G}']$.

The algebra $\mathbb{C}[\mathbb{G}']$ is semisimple and then isomorphic to a product of ℓ matrix algebras where ℓ is the number of conjugacy classes in $\mathbb{G}'$. So $\ell = |\mathbb{G}'| = m$ since $\mathbb{G}'$ is commutative. A dimension argument (or commutation argument) show that all the matrix algebras have to be of dimension 1. Finally $\mathbb{C}[\mathbb{G}'] \simeq \mathbb{C}^m$.

Moreover, we also have $\mathbb{C}[\mathbb{Z}^r] \simeq \mathbb{C}[{X_1}^{\pm 1}, \ldots, {X_r}^{\pm 1}]$ whose unique finite-dimensional subalgebra is $\mathbb{C}$.

Finally, we obtain $\mathbb{C}[\mathbb{G}] \simeq \mathbb{C}[{X_1}^{\pm 1}, \ldots, {X_r}^{\pm 1}]^m$. This implies that the finite-dimensional subalgebras of $\mathbb{C}[\mathbb{G}]$ are the subalgebra of $\mathbb{C}^m$. There thus exists only finitely many such subalgebras. □

Lemma 6.3. *Let $\mathbb{G}$ be a finitely generated group. Then $\mathbb{C}[\mathbb{G}]$ can be identified with a subalgebra of a Banach algebra over $\mathbb{C}$.*

Proof. Let us consider on $\mathbb{C}[\mathbb{G}]$ the norm defined by

$$\| \sum_{g \in \mathbb{G}} \lambda_g e_g \| = \sum_{g \in \mathbb{G}} |\lambda_g| .$$

For $x, y \in \mathbb{C}[\mathbb{G}]$, we have $\|xy\| \leq \|x\|\|y\|$. The completion of $\mathbb{C}[\mathbb{G}]$ will then be a Banach algebra. □

Corollary 6.4 (Diderrich's theorem for groups)**.** *Consider A and B be two finite nonempty subsets of a group $\mathbb{G}$. Assume that A is commutative. Let $H := \{g \in G \mid gAB = AB\}$. Then*

$$|AB| \geq |A| + |B| - |H| .$$

Proof. Since AB belongs to the subgroup of $\mathbb{G}$ generated by the finite sets A and B, we can assume that G is finitely generated. Lemma 6.3 then shows that $\mathbb{C}[\mathbb{G}]$ satisfies $\mathbf{H}_{\mathrm{w}}$. We then apply Theorem 4.1 to $\overline{A}$ and $\overline{B}$ which consists of invertible elements in $\mathbb{C}[\mathbb{G}]$. We have $|A| = \dim_{\mathbb{C}} \overline{A}$, $|B| = \dim_{\mathbb{C}} \overline{B}$ and by Lemma 6.1, we have $|H| = \dim_{\mathbb{C}} \overline{H} = \dim_{\mathbb{C}} \mathcal{H}$ where $\mathcal{H} = \{x \in \mathbb{C}[G] \mid x\langle \overline{A}\, \overline{B}\rangle = \langle \overline{A}\, \overline{B}\rangle\}$. Since $\mathbb{C}[\mathbb{G}(A)] = \mathbb{A}[\overline{A}]$ admits a finite number of finite-dimensional subalgebras by Lemma 6.2, we are done. □

Remark 6.5. Observe that in the case of a commutative group $\mathbb{G}$, Lemma 6.3 is not necessary. Indeed, we may consider the commutative finitely generated group $\langle A \cup B\rangle$ whose group algebra verifies $\mathbf{H}_{\mathrm{w}}$ by Lemma 6.2.

Remark 6.6. Contrary to [6], we recover here the results for the groups without using any Galois correspondence arguments which would become problematic in the noncommutative case.

7. Monoid setting

Let M be a multiplicative monoid with neutral element 1. Its set of invertible elements is defined as

$$U(M) = \{x \in M \mid \exists y \in M, \quad xy = yx = 1\}.$$

We denote by $\mathbb{C}[M]$ its monoid algebra over $\mathbb{C}$. Given a nonempty set A in G, we define $\overline{A} = \{e_a \mid a \in A\}$ as in the case of a group algebra. Moreover, we also write

$$H_A = \{h \in M \mid hA = A\} \quad \text{and} \quad \mathcal{H}_l(A) = \{x \in \mathrm{k}[M] \mid x\overline{A} \subset \mathrm{k}\langle \overline{A}\rangle\}$$

for the left stabilizer of A in M and the left stabilizer of $\mathrm{k}\langle\overline{A}\rangle$ in $\mathrm{k}[M]$, respectively. It is clear that H_A is a submonoid of M and $\mathcal{H}_l(A)$ a subalgebra of $\mathrm{k}[M]$. Nevertheless, Lemma 6.1 does not hold in general when M is not a group as illustrated by the following example.

Example 7.1. *Consider M defined as the quotient of the free monoid $\{a,b\}^*$ (with neutral element the empty word) by the relations*

$$a^2 = b^2 = ab = ba.$$

Given $x \in M$, let $\ell(x)$ be the common length of the words of x regarded as a class in $\{a,b\}^*$. Then $\ell(xy) = \ell(x) + \ell(y)$ for any x, y in M. For $A = \{1, a, b\}$, we thus have $H_A = \{1\}$. Nevertheless, the subalgebra $\mathcal{H}_l(A)$ is not reduced to $\mathbb{C}$. One easily verifies that it coincides with the 2-dimensional subalgebra $\mathcal{H}_l(A) = \mathbb{C} \oplus \mathbb{C}x$ generated by $x = a - b$ with $x^2 = 0$.

7.1. **Finite monoids.** The Kneser theorem for abelian groups becomes false in commutative finite monoids even if we assume the subsets considered intersect non trivially the set of invertible elements. To see this, define a monoid M as the quotient of the free monoid $\{a,b\}^*$ (with neutral element the empty word) by the relations

$$a^2 = b^2 = ab = ba \text{ and } a^4 = a. \tag{11}$$

Then $M = \{1, a, b, a^2, a^3\}$ is finite. For $A = B = \{1, a, b\}$, we have yet $A^2 = \{1, a, b, a^2\}$ and $H_{AB} = \{1\}$ whereas

$$4 = \left|A^2\right| \not\geqslant 2\,|A| - |H_{AB}| = 5.$$

It is nevertheless possible to obtain a Hamidoune type theorem from our algebra setting.

Theorem 7.2. *Let M be a finite monoid and A a finite subset in M satisfying $A \cap U(M) \neq \emptyset$. Then, for any $0 < \lambda \leq 1$, the subalgebra $\mathcal{H}_\lambda$ of $\mathbb{C}[M]$ which is the unique atom containing 1 contains $\mathcal{H}_l(A)$ and verifies*

$$|BA| \geq \lambda\,|A| + |B| - \lambda \dim_{\mathbb{C}}(\mathcal{H}_\lambda) \quad \text{and} \quad \dim_{\mathbb{C}}(\mathcal{H}_\lambda) \geq |H_A|$$

for any finite subset B in M such that $B \cap U(M) \neq \emptyset$. In particular $\mathcal{H}_1$ verifies

$$|BA| \geq |A| + |B| - \dim_{\mathbb{C}}(\mathcal{H}_1) \quad \text{and} \quad \dim_{\mathbb{C}}(\mathcal{H}_1) \geq |H_A|\,.$$

Proof. Since M is finite, $\mathbb{C}[M]$ verifies $\mathbf{H}_{\mathrm{s}}$. We apply Corollary 5.2 to $\overline{A}$ and $\overline{B}$. We have $\dim_{\mathbb{C}}(\mathcal{H}_\lambda) \geq |H|$ because $\mathbb{C}[H] \subset \mathcal{H}_l(A) \subset \mathcal{H}_\lambda$. □

Remark 7.3.

(1) Contrary to the group setting, for A a finite subset in M, the subalgebra $\mathbb{A}[\overline{A}]$ of $\mathbb{C}[M]$ generated by $\overline{A}$ can admit an infinite number of finite-dimensional subalgebras. This is notably the case when A contains a (non invertible) element a generating a submonoid

$$\langle a\rangle = \{1, a, \dots, a^m, a^{m+1}, \dots, a^{m+r-1}\}$$

with $a^{m+r} = a^m$. Then $\mathbb{A}[\overline{A}]$ admits a subalgebra isomorphic to $\mathbb{C}[X]/(X^{m+r} - X^m)$. We get

$$\mathbb{C}[X]/(X^{m+r} - X^m) \simeq \mathbb{C}[X]/(X^r - 1) \times \mathbb{C}[X]/(X^m)$$

thus $\mathbb{C}[\overline{A}]$ has an infinite number of finite-dimensional subalgebras as soon $m > 3$ by Theorem 3.12. So we cannot state a general monoid version of the Diderrich-Kneser theorem from Theorem 4.6.

(2) But, we have the following version : let M be a monoid whose elements are right regular and A be a finite commutative subset of M and B a finite subset of M, then $|AB| + |H_{AB}| \geq |A| + |B|$. Indeed, M may not be a submonoid of a group, but A does since it is commutative. So $\mathbb{C}[\mathbb{A}(A)]$ is a subalgebra of a finitely generated commutative group and thus has only a finite number of subalgebra by Lemma 6.2. Moreover, adapting the proof of Lemma 6.3, we get that $\mathbb{C}[M]$ is a subalgebra of a Banach algebra. Finally, in this context Lemma 6.1 still holds, since $e_{g'a} \neq e_{g''a}$ if $g' \neq g''$ (using notation of Lemma 6.1). Therefore, we can apply Theorem 4.1.

(3) It is also possible to get from the monoid algebra $\mathbb{C}[M]$ monoid versions of Corollary 4.9 and Theorem 5.4. They are left to the reader. Here also we have to use finite-dimensional subalgebras of $\mathbb{C}[M]$ instead of submonoids of M.

7.2. **Finitely generated commutative monoids.** Let M be a finitely generated commutative monoid. Its monoid algebra $\mathbb{C}[M]$ is a finitely generated algebra (over $\mathbb{C}$). It thus can be written as $\mathbb{C}[X_1, \ldots, X_r]/I$ where I is an ideal of $\mathbb{C}[X_1, \ldots, X_r]$. We now give a sufficient condition on the components of the algebraic variety V defined by I to apply Theorem 4.1.

Assume that I is a radical ideal (or that $\mathbb{C}[M]$ is reduced) and that the irreducible components of V coincide with its connected components. Then in this case $\mathbb{C}[M]$ is a finite product of integral algebras, one for each irreducible component of V. Thus $\mathbb{C}[M]$ satisfies hypothesis $\mathbf{H}_{\mathrm{w}}$ and we can apply Theorem 4.1 because we know by Lemma 6.2 that it admits a finite number of finite dimensional subalgebras.

To prove that $\mathbb{C}[M]$ is a finite product of integral algebras, write $V = V_1 \cup \cdots \cup V_s$ where the V_i are the irreducible components of V. For a subset X of $\mathbb{C}^r$, write $I(X)$ for the ideal of $\mathbb{C}[X_1, \ldots, X_r]$ of polynomial vanishing on all $x \in X$. In particular, we have by using the Nullstellensatz that $I = I(V)$ since $\mathbb{C}[M]$ is reduced. We also get $I = I(V) = I(V_1) \cap \cdots \cap I(V_s)$. Moreover, since the V_i are the connected component of V, we have $V_i \cap V_j = \emptyset$ for $i \neq j$. The Nullstellensatz also ensures us that $I(V_i) + I(V_j) = \mathbb{C}[X_1, \ldots, X_r]$ (see [4], Chapter 1 p.20). The Chinese remainder theorem allows us to write

$$\mathbb{C}[M] = \mathbb{C}[X_1, \ldots, X_r]/I(V_1) \cap \cdots \cap I(V_r) = \mathbb{C}[X_1, \ldots, X_r]/I(V_1) \times \cdots \times \mathbb{C}[X_1, \ldots, X_r]/I(V_r)$$

where $\mathbb{C}[X_1, \ldots, X_r]/I(V_j)$ is an integral domain since V_j is irreducible.

References

[1] N. Bourbaki, *Algèbre, Chapitre 5, Théorème **6.1***, (1981).
[2] G. T. Diderrich, On Kneser's addition theorem in groups, Proc. Ams. **38** (1973), 443-451.
[3] S. Eliahou. and C. Lecouvey, On linear versions of some addition theorems, Linear Algebra and multilinear algebra, **57** (2009), 759-775.
[4] W. Fulton. *Algebraic Curves*, Benjamin/Cumming Publishing Company, Inc.
[5] D. Grynkiewicz. Structural additive theory, Developments in Mathematics, vol 30 (2013).
[6] X. D. Hou, K. H. Leung and Xiang. Q, A generalization of an addition theorem of Kneser, Journal of Number Theory **97** (2002), 1-9.
[7] Y. O. Hamidoune, On the connectivity of Cayley digraphs, Europ. J. Comb., **5** (1984), 309-312.
[8] X. D. Hou, On a vector space analogue of Kneser's theorem, Linear Algebra and its Applications **426** (2007) 214-227.
[9] F. Kainrath, On local half-factorial orders, in Arithmetical Properties of Commutative Rings and Monoids, Chapman & Hall/CRC, Lect. Notes. Pure Appl. Math. 241-316 (2005).
[10] J. H. B. Kemperman, On complexes in a semigroup, Indag. Math. **18** (1956), 247-254.
[11] S. Lang, *Algebra,* Graduate Texts in Mathematics, Springer-Verlag New York Inc (2005).
[12] C. Lecouvey, Plünnecke and Kneser type theorems for dimension estimates, Combinatorica, 34, (2014) 331-358.
[13] D. Mirandola, G. Zemor, Critical pairs for the product singleton bound, preprint 2015 arXiv: 150106419.

[14] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Text in Mathematics **165**, Springer-Verlag New York (1996).
[15] J. E. Olson, On the sum of two sets in a group, J. Number Theory **18** (1984), 110-120.
[16] I. Z. Ruzsa, Sumsets and structure, Combinatorial Number Theory and additive group theory, Springer New York (2009).
[17] T. Tao, Non commutative sets of small doublings, European Journal of Combinatorics **34** (2013), 1459-1465.
[18] T. Tao, Product set estimates for non-commutative groups, Combinatorica 28 (2009), 547-594.

Laboratoire de Mathématiques et Physique Théorique (UMR CNRS 6083)
Université François-Rabelais, Tours
Fédération de Recherche Denis Poisson - CNRS
Parc de Grandmont, 37200 Tours, France.

Univ. Orléans, MAPMO (UMR CNRS 7349), F-45067, Orléans, France
FDP - FR CNRS 2964